www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 04, April 2023, pp : 187-198

e-ISSN : 2583-1062

Impact Factor : 5.725

# BLOCKCHAIN-BASED SYSTEM AND METHODS FOR SENSITIVE DATA TRANSACTIONS

**S. Yuvaraj[1], Ms. Sarika Jain[2], Dr. S. Geetha[3]**

[1]M.Sc – CFIS, Department of Computer Science and Engineering, Dr. M.G.R Educational and Research Institute, Chennai 600 095, Tamilnadu, India

[2]Center of Excellence in Digital Forensics, Perungudi, Chennai 600 089, Tamilnadu, India

[3]Head of the Department, Department of Computer Science and Engineering, Dr. M.G.R Educational and Research Institute, Chennai 600 095, Tamilnadu, India

## ABSTRACT

A blockchain-based processing framework for sensitive data is proposed. The underlying blockchain module provides technical support, such as virtual machines, consensus algorithms, transaction verification mechanisms, and accounting mechanisms. The E-contract layer module provides a distributed application service and uses the blockchain technology to support it. The proposed smart system is used by each party get involved in the production of sensitive data. The final sensitive data are produced by the final data generator, and other modules involved in the process of data production are unaware of the final data. This approach prevents the leakage of sensitive data into the circulation.

## 1. INTRODUCTION

Sensitive data transaction is confidential information that must be kept safe and out of reach from all outsiders unless they have permission to access it. Access to sensitive data should be limited through sufficient data security and information security practices designed to prevent data leaks and data breaches. Sensitive data can be any sort of information that needs to be protected from unauthorized access to safeguard the privacy or security of an individual or organization. It can include any information pertaining to: Passwords. Encryption keys.

**Objectives**

Collecting staff information and maps their relationships for a complete picture of user account organization. We'll help you with privacy design when creating users, groups, and role-based permissions Encryption is a very generic term and there are many ways to encrypt data. Companies need to implement and manage encryption correctly. The key to a good encryption strategy is using strong encryption and proper key management. Encrypt sensitive data before it is shared over untrusted networks (ex. Encrypted file storage).

## 2. LITERATURE SURVEY

**Dongjie Liu et.al,** although a variety of techniques to detect malicious websites have been proposed, it becomes more and more difficult for those methods to provide a satisfying result nowadays. Many malicious websites can still escape detection with various Web spam techniques. In this paper, we summarize three types of Web spam techniques used by malicious websites, such as redirection spam, hidden IFrame spam, and content hiding spam. We then present a new detection method that adopts the perspective of users and takes screenshots of malicious webpages to invalidate Web spams. The proposed detection method uses a Convolutional Neural Network, which is a class of deep neural networks, as a classification algorithm. In order to verify the effectiveness of the method, two different experiments have been conducted. First, the proposed method was tested based on a constructed complex dataset. We present comparison results between the proposed method and representative machine learning-based detection algorithms. Second, the proposed method was tested to detect malicious websites in a real-world Web environment for three months. These experimental results illustrate that the proposed method has a better performance and is applicable to a practical Web environment.

**Paul J. Taylor et.al,** since the publication of Satoshi Nakamoto's white paper on Bitcoin in 2008, blockchain has (slowly) become one of the most frequently discussed methods for securing data storage and transfer through decentralized, trustless, peer-to-peer systems. This research identifies peer-reviewed literature that seeks to utilize blockchain for cyber security purposes and presents a systematic analysis of the most frequently adopted blockchain security applications. Our findings show that the Internet of Things (IoT) lends itself well to novel blockchain applications, as do networks and machine visualization, public key cryptography, web applications, certification schemes and the secure storage of Personally Identifiable Information (PII). This timely systematic review also sheds light on future directions of research, education and practices in the blockchain and cyber security space, such as security of blockchain in IoT, security of blockchain for AI data, and sidechain security, etc.

**Keiic Keiichi Iwamura et.al,** typically, unconditionally secure computation using a $(k, n)$ threshold secret sharing is considered impossible when $n< 2k - 1$. Therefore, in our previous work, we first took the approach of finding the conditions required for secure computation under the setting of $n< 2k - 1$ and showed that secure computation using a $(k, n)$ threshold secret sharing can be realized with a semi-honest adversary under the following three preconditions: (1) the result of secure computation does not include 0; (2) random numbers reconstructed by each server are fixed; and (3) each server holds random numbers unknown to the adversary and holds shares of random numbers that make up the random numbers unknown to the adversary. In this paper, we show that by leaving condition (3), secure computation with information-theoretic security against a semi-honest adversary is possible with $k \leq n< 2k - 1$. In addition, we clarify the advantage of using secret information that has been encrypted with a random number as input to secure computation. One of the advantages is the acceleration of the computation time. Namely, we divide the computation process into a preprocessing phase and an online phase and shift the cost of communication to the preprocessing phase. Thus, for computations such as inner product operations, we realize a faster online phase, compared with conventional methods.

**Nileshkumar Kakade et.al,** secret sharing is an important means to achieve confidentiality and data privacy. Secret sharing deals with splitting a secret information with various players. The goal of the secret sharing is security of secret, privacy and hiding information. There are numerous techniques available for secret sharing e.g., polynomial, Chinese remainder theorem, vector space, matrix projection. Techniques have characteristics like threshold, proactive, verifiable. Proactive secret sharing scheme allow user to change share in case of doubt of theft. In this work we propose the proactive secret sharing scheme based on homomorphic techniques. Our scheme consists of three phases of share construction, share renewal, share reconstruction. Central authority splits an encrypted secret with each parties using homomorphic property of paillier encryption i.e., subtraction. In renewal process two or more parties relate share with each other for to generated renewed share. In reconstruction process all parties share will be add to central authority then encrypted secret will be generated. Central authority will decrypt encrypted secret using secret key then original secret will be generated. Our schemes unique features are share can be renewed any time, each party can choose secret of their own choice, if any two parties have same content share, then also encrypted share will be different due to non-deterministic property of paillier encryption.

**Sundari S et.al,** secure multiparty computation (SMC) is needed now-a-days in which data are distributed between different parties. Moreover, organizations are wished to collaborate with other parties who conduct same business, for their mutual benefits. SMC provides users to gain much information from the larger data without disclosing the data. This project combines the technique secure multi-party computation and the differential privacy for vertically partitioned data between parties. To achieve this, a multi-party protocol has been proposed for the exponential mechanism. Reliable access to data is must for most computer applications and data servers. Some factors cause unauthorized access to stored data. Two Phase Validation (2PV) provides the authentication for the users, while integrating the data in multiparty computation. Data can get corrupted due to some malfunctions. Disk errors are common today but the storage technologies are not designed to handle such kind of errors. A simple integrity violation is detected by the higher-level software which causes further loss of data. The proposed system is to verify the integrity of random subsets of data against general or malicious corruptions through Distributed Data Integrity (DDI) Protection.

## 3. EXISTING SYSTEM

**Concept**

Most of the existing homomorphic secret sharing and secure multi-party computing technologies have the problems of massive communication rounds and too much traffic load.

**Technique**

Different Hash Function Model.

**Disadvantage**

It takes long time to process various hash function methods.

## 4. PROPOSED SYSTEM

**Concept**

The proposed smart system is used by admin or authority get involved in the production of sensitive data. The final sensitive data are produced by the final data administrator or authority person, and other modules involved in the process of data aggregation are unaware of the final data.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 04, April 2023, pp : 187-198

e-ISSN : 2583-1062

Impact Factor : 5.725

**Technique**

RSA (Rivest, Shamir, Adleman) and AES (Advanced Encryption Standard) algorithm.

**Advantage**

It gives standard and valid solution to process the data with has function.

## 5. MODELLING AND ANASLYSIS

**Modules**

- Staff
- Team Leader
- Management

**Module Explanation**

**Staff**

The register module provides a conceptual framework for entering data on those staff in a way that: eases data entry & accuracy by matching the staff entry to the data source (usually paper files created at point of care), ties easily back to individual staff records to connect registers to staff data, and collects data elements to enable better supervision of donation programs. Here symbolizes a unit of work performed within a database management system (or similar system) against a database, and treated in a coherent and reliable way independent of other transactions. A transaction generally represents any change in database user will transfer the amount to provider. In this module the staff will also view the team leader added file. And analysis the details will be responsible for your file stored in database. The staff to Request for download file with the land longitude and the user will update the report along with their opinion and they will be stored the database. In this module the staff download the file after management accept the request. It will be stored on local storage.

**HOD**

In this module in our project, here symbolizes a unit of work performed within a database management system (or similar system) against a database, and treated in a coherent and reliable way independent of other transactions. A transaction generally represents any change in database user will transfer the amount to provider. The team leader can then select a file from their computer and click the upload button to submit the file to the server. The Java file upload Servlet will then capture that file and persist. It will be stored in database. The staff add the file to the staffs. The data directly stored in database. Then staff will view the uploaded file.

**Management**

In this module in our project, here symbolizes a unit of work performed within a database management system (or similar system) against a database, and treated in a coherent and reliable way independent of other transactions. A transaction generally represents any change in database user will transfer the amount to provider. The register module provides a conceptual framework for entering data on those team leader in a way that: eases data entry & accuracy by matching the team leader entry to the data source (usually paper files created at point of care), ties easily back to individual team leader records to connect registers to team leader data, and collects data elements to enable better supervision of team programs. In this module the management generate key for the staff request. Because the key for the security purpose. After get the key from management the staff will download the file with key. the management will response the data file fully analyzed data in category wise view management will be responsible for your file stored in database.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

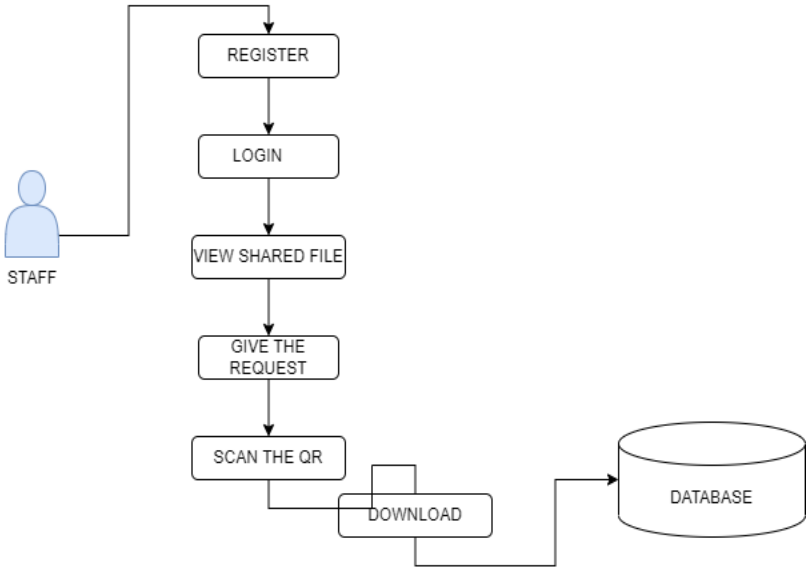
Vol. 03, Issue 04, April 2023, pp : 187-198

e-ISSN : 2583-1062

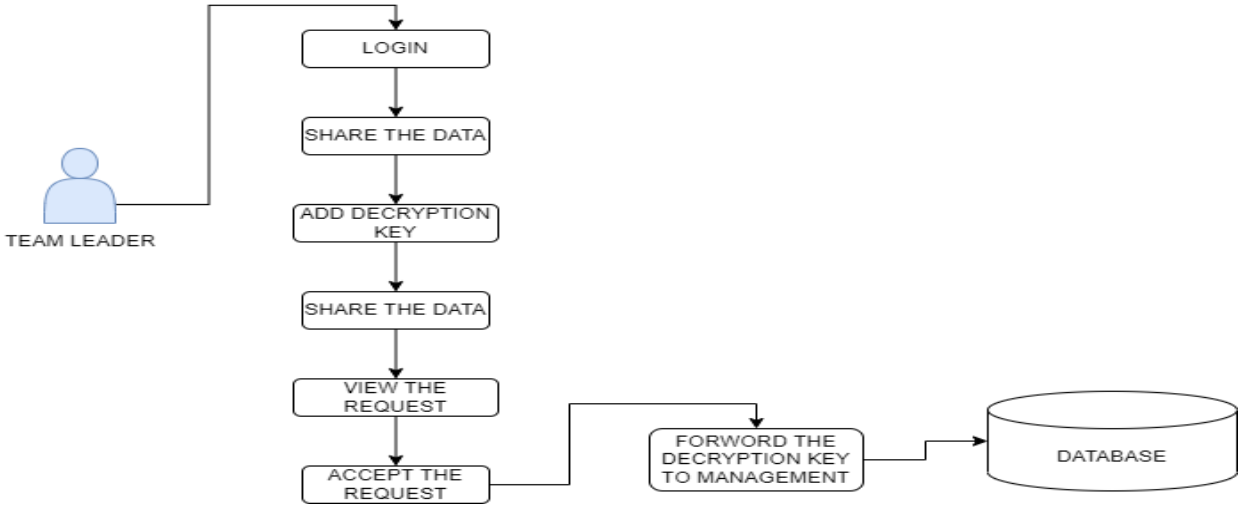
Impact Factor : 5.725

**Module Diagram**

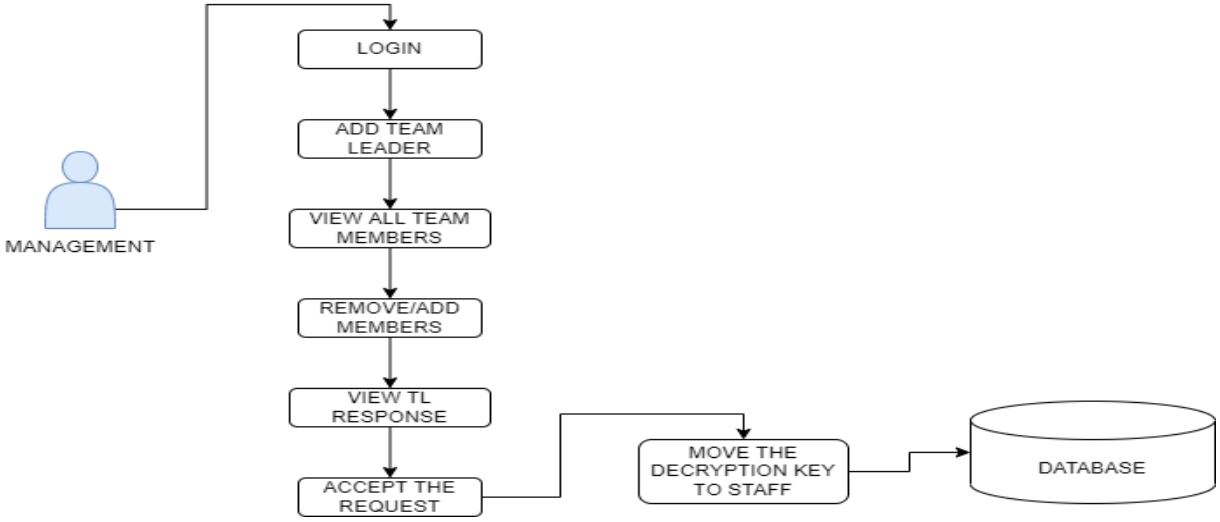
**Staff**




**HOD**




**Management**



www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 04, April 2023, pp : 187-198

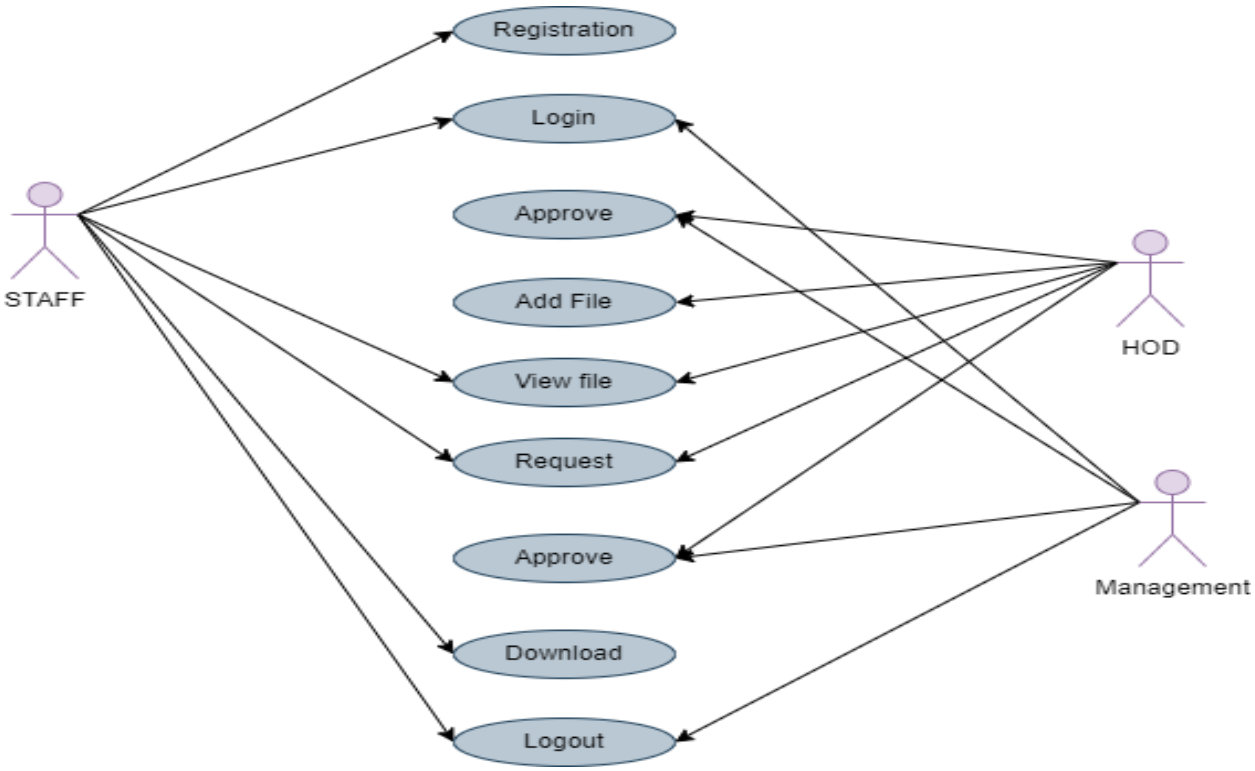
e-ISSN : 2583-1062

Impact Factor : 5.725

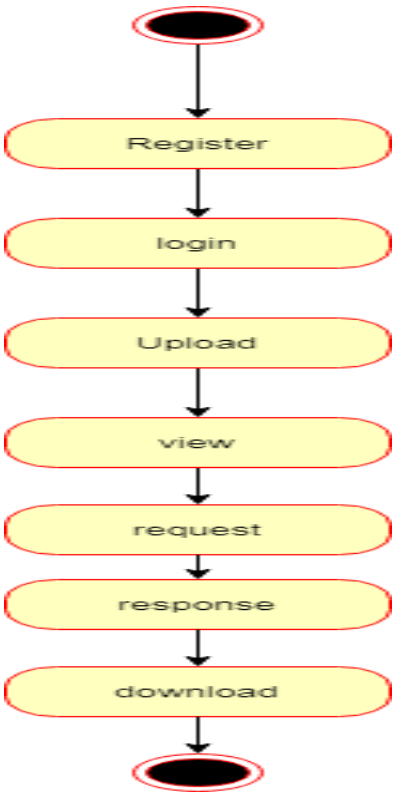
**Design Engineering**

**General**

**Use Case**




State Diagram



INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

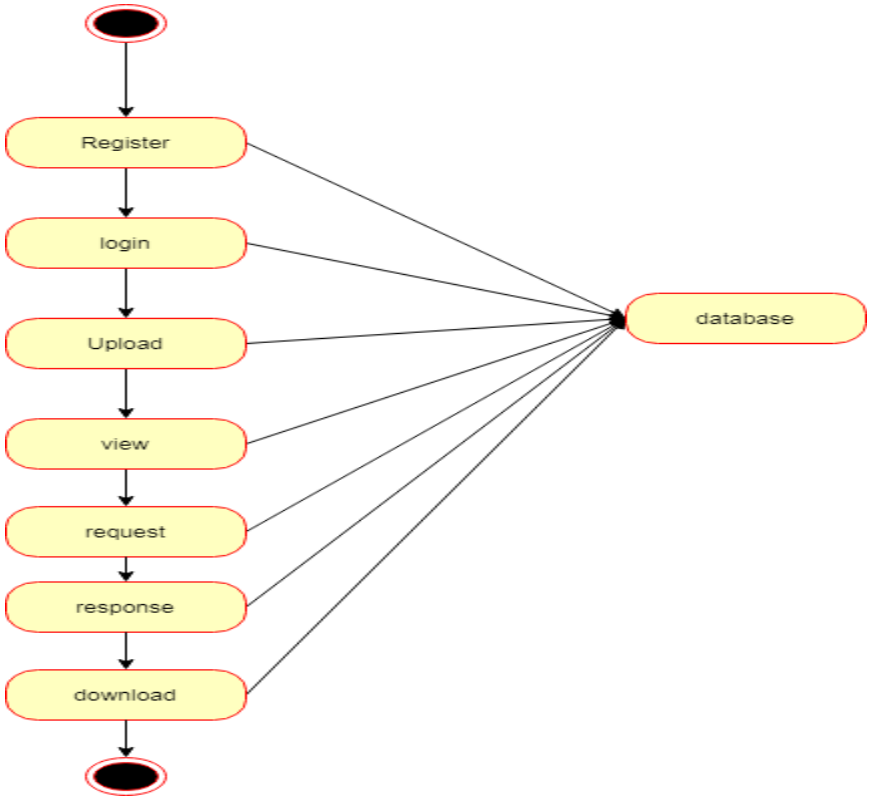
www.ijprems.com
editor@ijprems.com

Vol. 03, Issue 04, April 2023, pp : 187-198

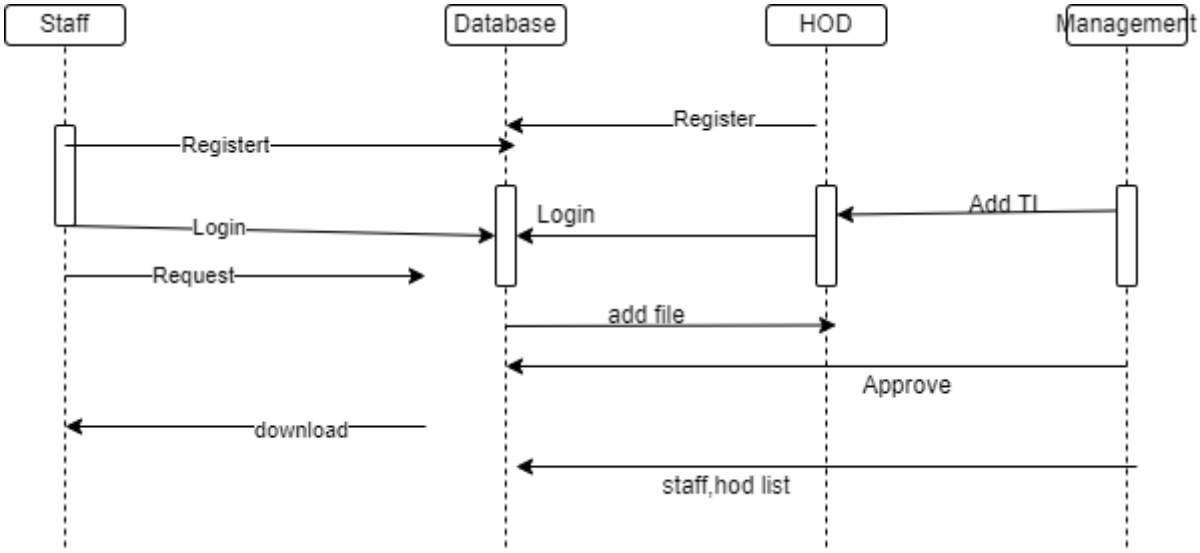
e-ISSN : 2583-1062

Impact Factor : 5.725

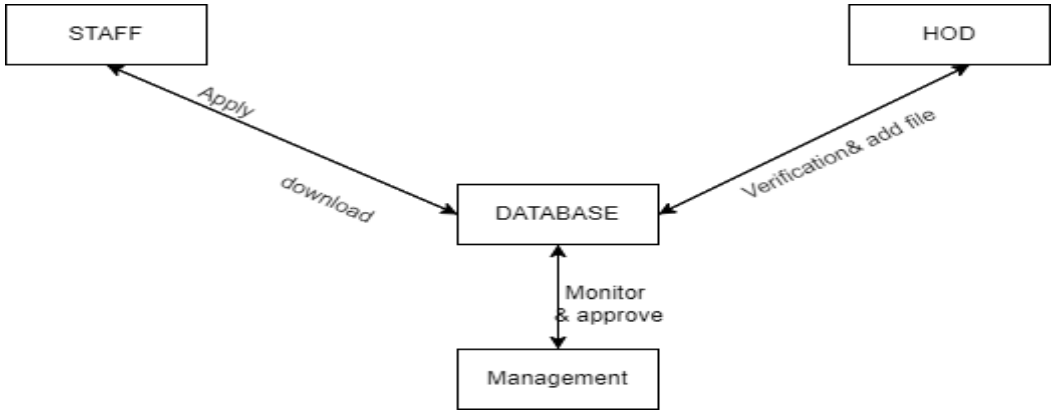
Activity Diagram




Sequence Diagram




Collaboration Diagram:



INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

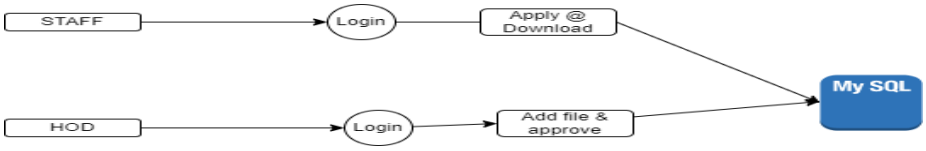
Vol. 03, Issue 04, April 2023, pp : 187-198

e-ISSN : 2583-1062

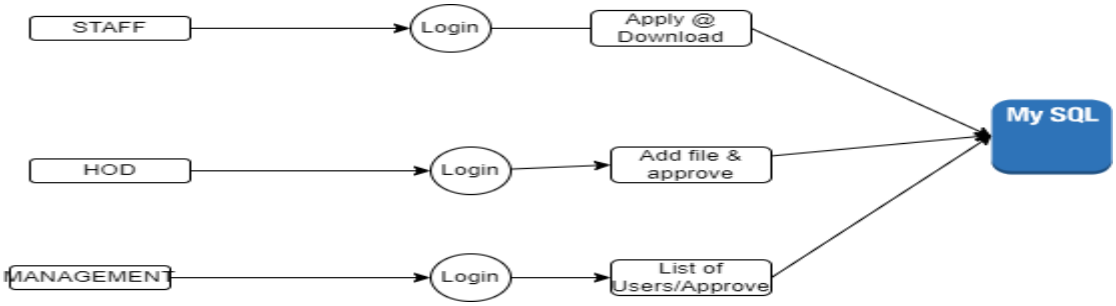
Impact Factor : 5.725

Data Flow Diagram

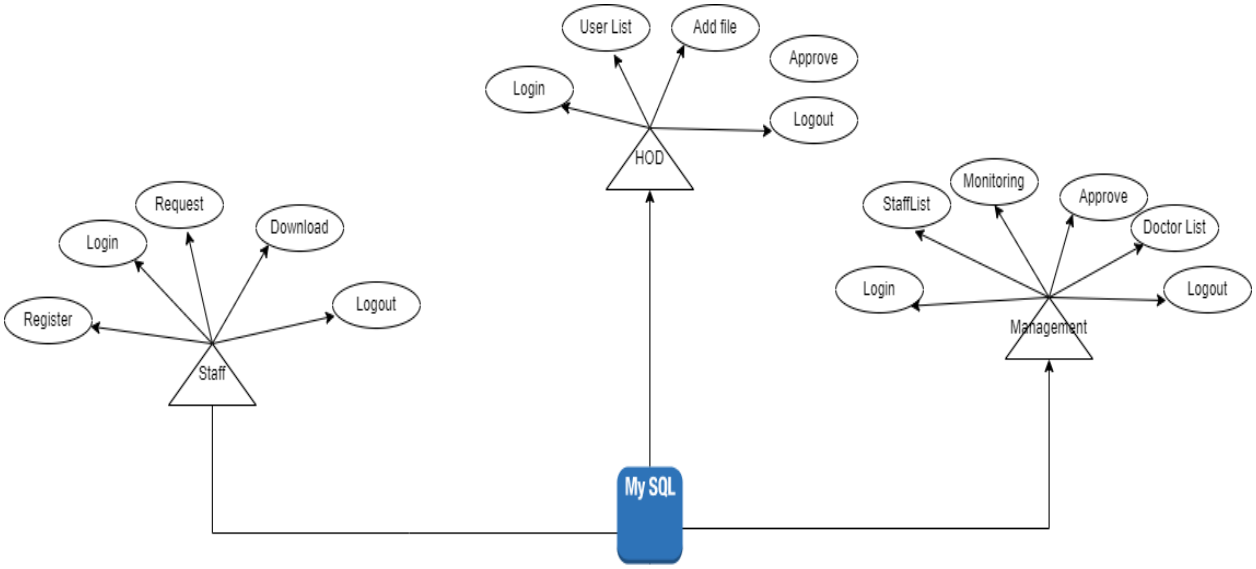
Level 1



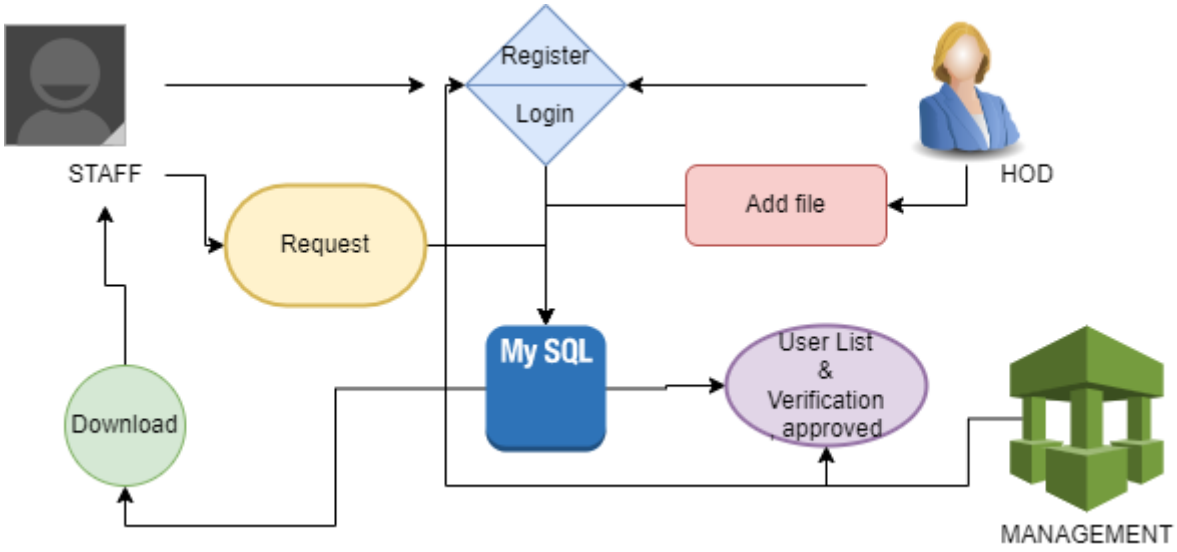

Level 2




E-R Diagram




System Architecture



www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

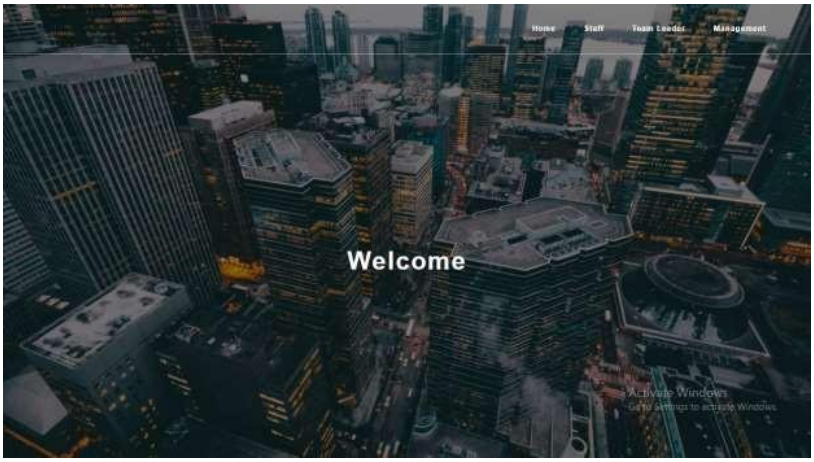
Vol. 03, Issue 04, April 2023, pp : 187-198

e-ISSN : 2583-1062

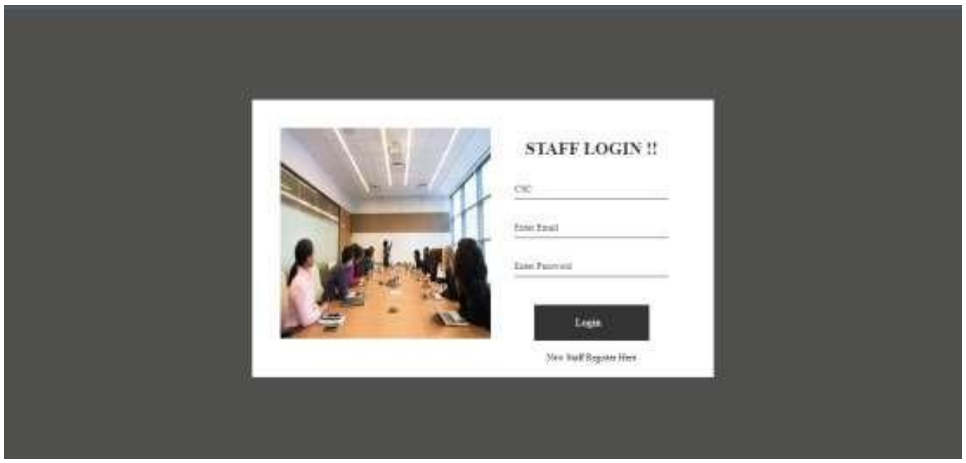
Impact Factor : 5.725

**Snapshots**

**Home Page**




Staff Login Page




HOD login page

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 04, April 2023, pp : 187-198

e-ISSN : 2583-1062

Impact Factor : 5.725

**Management Login Page**


Management page


**HOD Add Page**

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

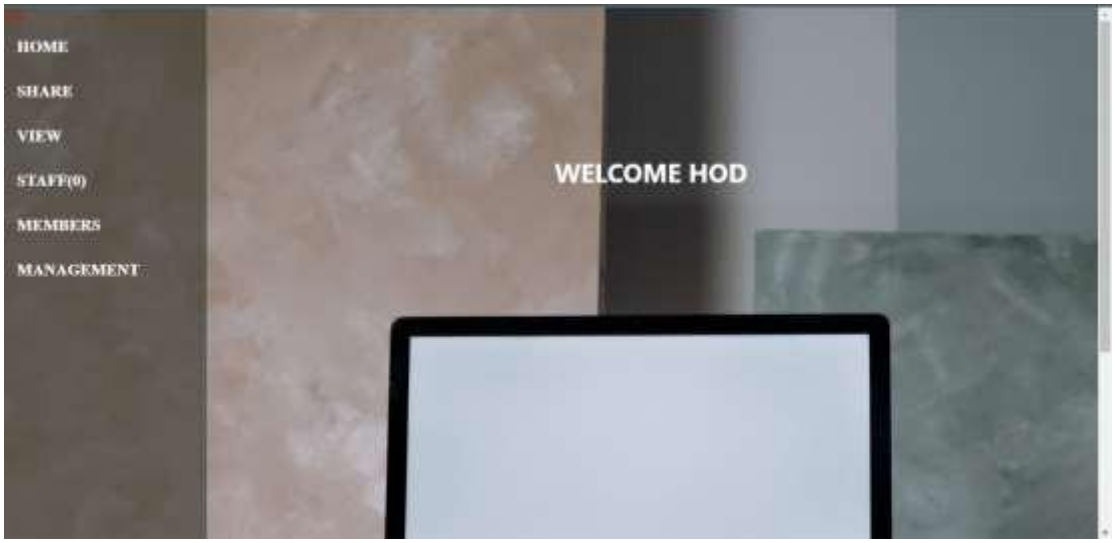
Vol. 03, Issue 04, April 2023, pp : 187-198

e-ISSN : 2583-1062

Impact Factor : 5.725


**Management Accept View Page**


**HOD Login Page**




www.ijprems.com
editor@ijprems.com

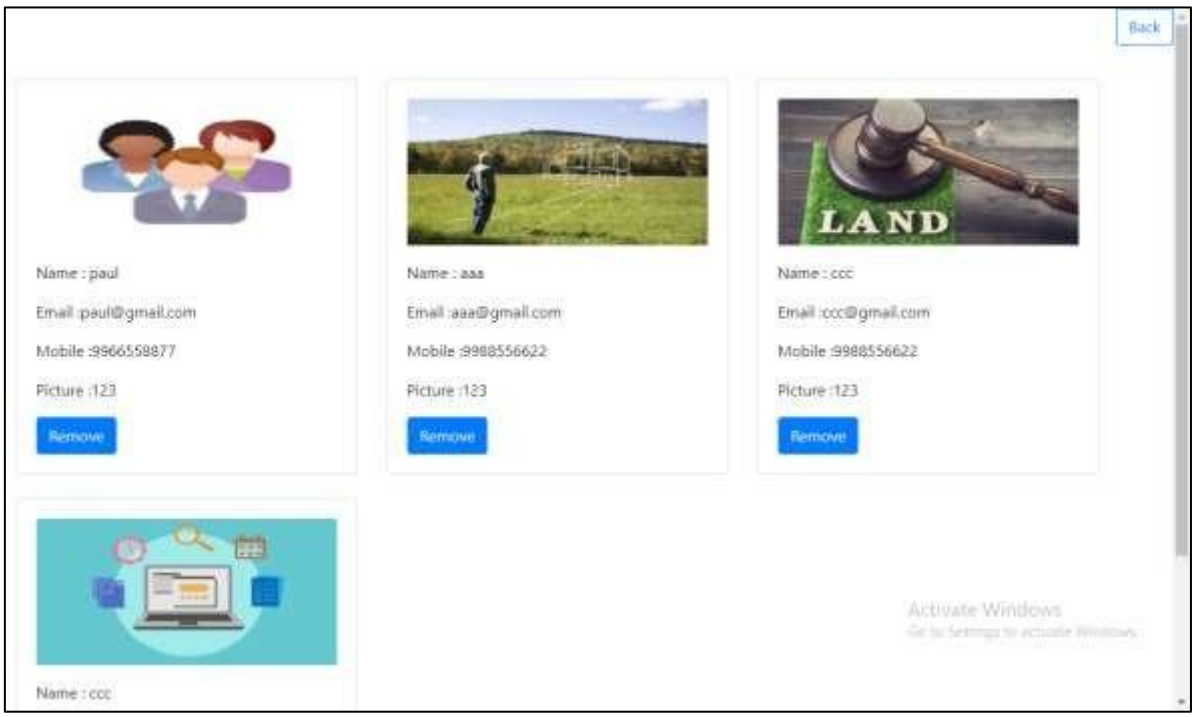
INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

Vol. 03, Issue 04, April 2023, pp : 187-198

e-ISSN : 2583-1062

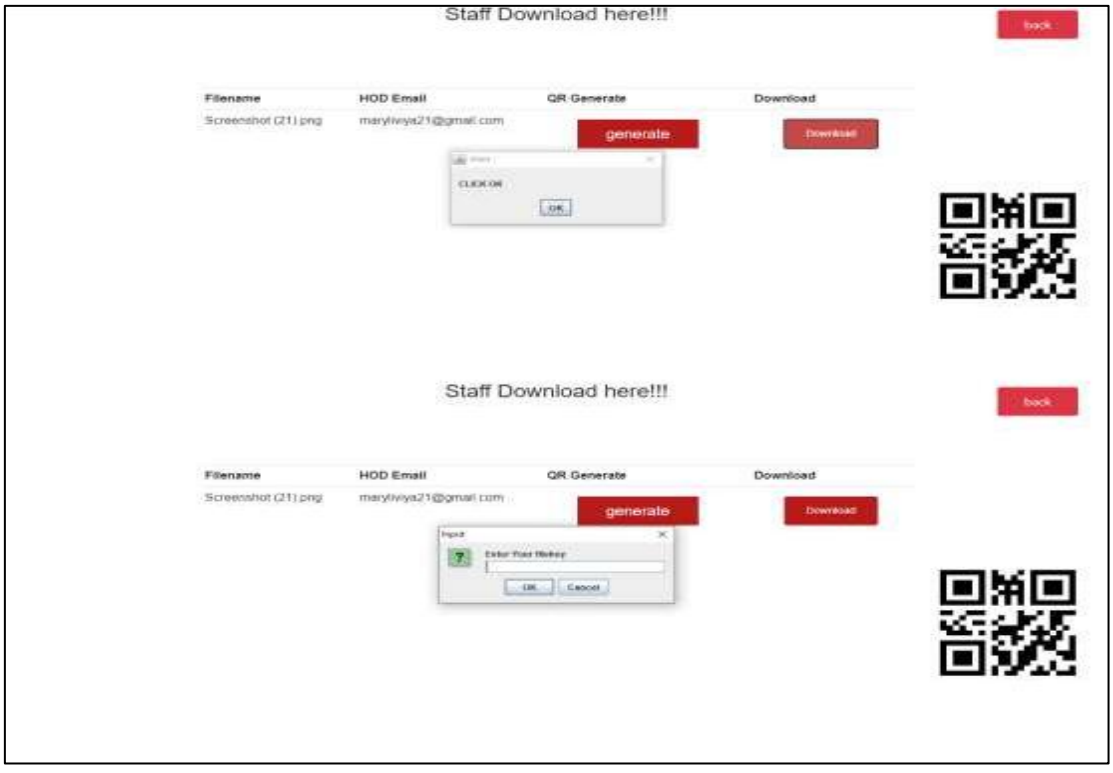
Impact Factor : 5.725

**Members List**





**Employee Download Page**




## 6. CONCLUSIONS

Data sensitivity concerns information that should be protected from unauthorized access or disclosure due to its sensitive nature. for some, that might be team leader, staff details records. Sensitive data is confidential information

that must be kept safe and out of reach from all outsiders unless they have permission to access it. Access to sensitive data should be limited through sufficient data security and information security practices designed to prevent.

## 7. REFERENCES

[1] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K. K. R. Choo, "A systematic literature review of blockchain cyber security," Digital Communications and Networks, vol. 6, no. 2, pp. 147-156, 2020.

[2] D. Liu and J. Lee, "CNN based Malicious Website Detection by Invalidating Multiple Web Spams," IEEE Access, vol. 8, no. 1, pp. 97258-97266, 2020.

[3] W. Martin, V. Friedhelm, and K. Axel, "Tracing manufacturing processes using blockchain-based token compositions," Digital Communications and Networks, vol. 6, no 2, pp. 167-176, 2019.

[4] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos and G. Das, "Everything You Wanted to Know About the Blockchain: Its Promise, Components, Processes, and Problems," IEEE Consumer Electronics Magazine, vol. 7, no. 4, pp. 6-14, 2018.

[5] L. Peng, W. Feng, and Z. Yan. (2020). Privacy preservation in permissionless blockchain: A survey. Digital Communications and Networks. [Online]. Available: https://doi.org/10.1016/j.dcan.2020.05.008.

[6] N. Kakade and U. Patel, "Secure Secret Sharing Using Homomorphic Encryption," in Proc. 2020 11th International Conference on Computing, Communication and Networking Technologies, 2020, pp. 1-7.

[7] S. Sundari and M. Ananthi, "Secure multi-party computation in differential private data with Data Integrity Protection," in Proc. 2015 International Conference on Computing and Communications Technologies, 2015, pp. 180-184.

[8] S. Jiao, T. Lei, Y. Gao, Z. Xie and X. Yuan, "Known-Plaintext Attack and Ciphertext-Only Attack for Encrypted Single-Pixel Imaging," IEEE Access, vol. 7, no.2, pp. 119557-119565, 2019.

[9] S. Kaushik, and S. Puri, "Online transaction processing using enhanced sensitive data transfer security model," in Proc. 2012 Students Conference on Engineering and Systems, 2012, pp. 1-4.

[10] W. Zheng, Z. Zheng, X. Chen, K. Dai, P. Li and R. Chen, "NutBaaS: A Blockchain-as-a-Service Platform," IEEE Access, vol. 7, pp. 134422-134433, 2019.

[11] F. Casino and C. Patsakis, "An Efficient Blockchain-Based Privacy-Preserving Collaborative Filtering Architecture," IEEE Transactions on Engineering Management, vol. 67, no. 4, pp. 1501-1513, Nov. 2020.

[12] D. Chkliaev, J. Hooman and P. van der Stok, "Mechanical verification of transaction processing systems," in Proc. ICFEM 2000. Third IEEE International Conference on Formal Engineering Methods, 2000, pp. 89-97.

[13] S. Zhang, and J H. Lee. "Mitigations on Sybil-based Double-spend Attacks in Bitcoin," IEEE Consumer Electronics Magazine, vol.7, no. 2, pp. 1-1, 2020.

[14] X. Wang, Q. Feng and J. Chai, "The Research of Consortium Blockchain Dynamic Consensus Based on Data Transaction Evaluation," in Proc. 2018 11th International Symposium on Computational Intelligence and Design, 2018, pp. 214-217.

[15] S. Zhang, and J. H. Lee, "A group signature and authentication scheme for blockchain-based mobile-edge computing," IEEE Internet of Things Journal, vol. 7, no. 5, 4557-4565, 2019.