

Blockchain based Authentication Scheme to Secure IoT Devices

Mrs. Juslin F¹, Ms. Anupama Shetter² and Ms. Tejaswini E³

¹⁻³ATME College of Engineering/Electronics and Communication Engineering Department, Mysuru, India
Email: juslinfranklin@gmail.com, anupamashetter@gmail.com, tejaswinie2000@gmail.com

Abstract—The IoT offers enormous opportunities and brings some challenges. Authentication considered one of the main challenges introduced by IoT. IoT devices are not able to protect themselves due to their limited processing and storage capabilities. Researchers proposed authentication algorithms with either a lack of scalability or vulnerable to cyberattacks. In this paper, we propose a decentralized token-based authentication based on fog computing and block chain. The protocol provides a secure authentication protocol using access token, ECC cryptography, and block chain as decentralized identity storage. The block chain uses cryptographic identifiers, records immutability, and provenance, which allows the implementation of a decentralized authentication protocol. These features ensure a light and secure identity management system. We evaluate this protocol communication between controller, gateways, and devices using AVISPA/ HLPSL, and results obtained from AVISPA simulation shows that our protocol is safe based on secrecy and strong authentication criteria. The paper uses four test cases to test the Ethereum smart contract implementation to ensure the system functions properly.

Index Terms— Cohesive soil, Rice husk ash, Metakaolin and Cement.

I. INTRODUCTION

In a Block-Chain IOT environment, when data or device authentication information is put on a block chain, personal information may be leaked through the proof-of-work process or address search. In this project, we apply Zero-Knowledge proof to a strong room system that proves without disclosing information such as public key, and we have studied how to enhance anonymity of block chain for privacy protection.

This application is uses block chain to prevent security threats such as data counterfeiting, which could occur using strong rooms. Zero-Knowledge proof, block chain anonymity enhancement technology, was introduced to prevent security threats such as personal information infringement through block inquiry. It was proposed to use smart contracts to prevent strong room data forgery and personal information.

This project is about adding a security protocol layer to the process of accessing the IOT devices. The existing protocols do not implement the security so stringently. Earlier protocols lack security in that the security is restricted to a single username and password. A compromise of the username or password may result in misuse of the IOT resources.

II. LITERATURE SURVEY

National Chung Cheng University, Taiwan (February 7-8, 2020) and Chitkara University. India (February 14-15,

2020) Published by Indo - Taiwan 2nd International Conference on Computing, Analytics and Networks (Indo-Taiwan ICAN 2020). This paper presents. researchers categorized IoT security issues into a low level, high level, and intermediate level. Authentication, secure communication, replay attacks, jamming adversaries, Sybil attack, and related security issues have been raised by the researchers A variety of authentication mechanisms such as passwordbased, Onetime password-based, the smart card-based, certificate- based have been proposed in the literature [1].

etal, Deepak, Rajiv Ranjan, and Jinjun Chen. "Big Data Stream Security Classification for IoT Applications." (2019). In this paper, analyses the security aspects in a novel Cloud architecture for Big Stream applications, which efficiently handles Big Stream data through a Graph-based platform and delivers processed data to consumers, with low Olatency. The authors detail each module defined in the system architecture, describing allo refinements required to make the platform able to secure large data streams. An experimentation is also conducted in order to evaluate the performance of the proposed architecture when integrating security mechanisms [3].

Khan, Minhaj Ahmad, and Khaled Salah. "IoT security: Review, blockchain solutions, and open challenges." *Future generation computer systems* 82 (2018): 395 411. This paper, present and survey major security issues for IoT. We review and categorize popular security issues with regard to the IoT layered architecture, in addition to protocols used for networking, communication, and management [4].

Krishnan, K. Navaneeth. et al. "Blockchain based security framework for IoT implementations." 2018 International CET Conference on Control, Communication, and Computing (IC4). IEEE, 2018. This article presents a new framework named ANDROSCANREG (Android Permissions Sean Registry) that allows to extract and analyses the requested permissions in an Android application via a decentralized and distributed system. This framework is based on the emerging technology Blockchain whose potential is approved in the matter of transparency, reliability, security, and availability without resorting to a central processing unit judged of trust [5]

Guan, Zhitao, et al. "APPA: An anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT." *Journal of Network and Computer Applications* 125 (2019): 82-92. In APPA scheme, the anonymity and authenticity of the device is guaranteed with pseudonym and pseudonym certificate, which can be updated autonomously. Taking the advantage of a local certification authority, the pseudonym management can be shifted to specialized fogs at the network edge, which provide real-time service for device registration and update [6].

Tharani, Jeyakumar Samantha, Mukunthan Tharmakulasingant and Vallipuram Muthukkumarasamy. "A blockchainbased database management system." *The Knowledge Engineering Review* 35 (2020). This paper described the database management system using blockchain technology that can be used by any software applications. The blockchain database connected to the cloud server can be used to increase the trustfulness of the application. [7].

Almadhoun, Randa, et al. "A user authentication scheme of IoT devices using blockchain-enabled fog nodes." 2018 IEEE/ACS 15th international conference on computer systems and applications (AICCSA) IEEE, 2018. This paper demonstrates the effectiveness of FogBus by creating a computing environment with it that integrates finger pulse oximeters: as IoT devices with Smartphone-based gateway and Raspberry Pi-based Fog nodes for Sleep Apnea analysis. [8].

Yaga, Dylan, et al. "Blockchain technology overview." *arXiv preprint arXiv:1906.11078* (2019). This paper aim is to analyze conveniences and difficulties, related to the Blockchain integration and implementation in the different fields of modern industry. The Blockchain is the newest and perspective technology in modern economy [9].

Tariq, Noshina, et al. "The security of big data in fog-enabled IoT applications including blockchain: A survey." *Sensors* 19.8 (2019): 1788. This paper aims to improve understanding the challenges to secure future digital infrastructure while it is still evolving. After introducing the infrastructure generating big data, the functionality-based fog architecture is defined. In addition, a comprehensive review of security requirements in fog enabled IoT systems is presented. Then, an in-depth analysis of the fog computing security challenges and big data privacy and trust concerns in relation to fog-enabled IoT are given.[11]

III. OBJECTIVE

We implement the security process as a middleware. The aim of the project is to introduce a layer of security between the user and IOT server. In addition to cryptographic artifacts like private keys and public keys, a further layer of security is introduced by involving certificates. The public key is used to encrypt the data and the

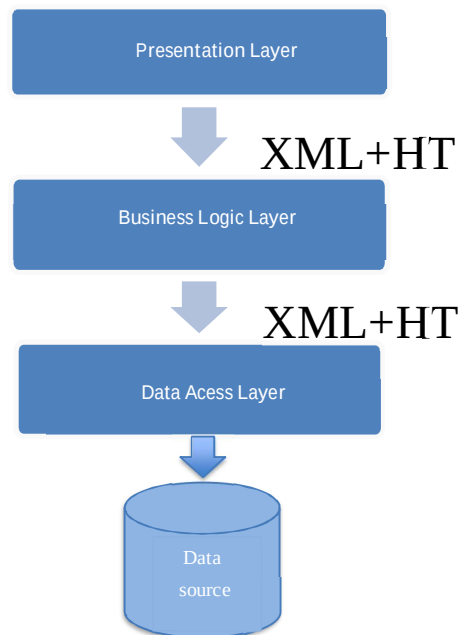
private key is used to decrypt the data. Once authenticated, the server creates a session for the user. The session may typically last around 30-40 seconds. Within this timeout period, user can communicate with the IOT device. The user can pass commands to read, write, turn on, turn off etc.

IV. METHODOLOGY

The purpose of the design phase is to plan a solution of the problem specified by the requirements document. This phase is the first step in moving from the problem domain to the solution domain. In other words, starting with what is needed; design takes us toward how to satisfy the needs. The design of a system is perhaps the most critical factor affecting the quality of the software; it has a major impact on the later phases particularly testing and maintenance.

A. Three Tier Architecture

Three-tier architecture is a client-server architecture in which the functional process logic, data access, computer data storage and user interface are developed and maintained as independent modules on separate platforms. Three-tier architecture is a software design pattern and well-established software architecture. Three-tier architecture allows any one of the three tiers to be upgraded or replaced independently. The user interface is implemented on a desktop PC and uses a standard graphical user interface with different modules running on the application server. The relational database management system on the database server contains the computer data storage logic. The middle tiers are usually multi-tiered.



The three tiers in three-tier architecture are:

Presentation Tier: Occupies the top level and displays information related to services available on a website. This tier communicates with other tiers by sending results to the browser and other tiers in the network.

Application Tier: Also called the middle tier, logic tier, business logic or logic tier, this tier is pulled from the presentation tier. It controls application functionality by performing detailed processing.

Data Tier: The **data tier** is responsible for storing the application's data and sending it to the business tier when requested.

B. Data Flow Diagrams (DFD)

On a Data Flow Diagram, data items flow from an external data source or an internal data store to an internal data store or an external data sink, via an internal process. A DFD provides no information about the timing of processes, or about whether processes will operate in sequence or in parallel. It is therefore quite different from a Flowchart. Which shows the flow of control through an algorithm, allowing a reader to determine what

operations will be performed, in what order, and under what circumstances, but not what kinds of data will be input to and output from the system, nor where the data will come from and go to, nor where the data will be stored.

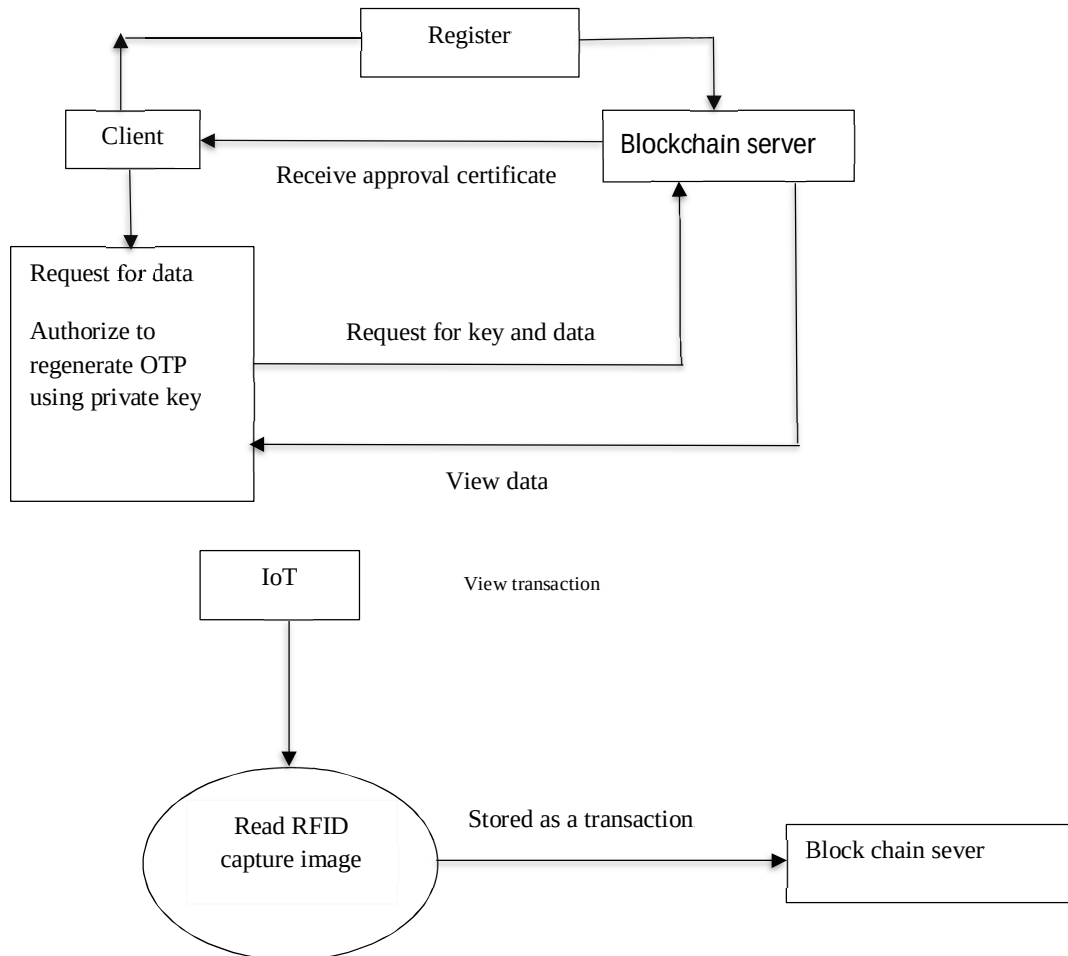


Fig: Data flow diagram for block chain server

C. Data Flow Diagrams

Processes: A process transforms data values. The lowest processes are our functions without side effects.

Data Flows: A data flow connects the output of an object or process to the input of another object or process. It represents the intermediate data values within the computation. It is drawn as an arrow between the procedure and the consumer of the data value. The arrow is labeled with the description of the data, usually its name or type.

Actors: An actor is an active object that drives the data flow graph by producing or consuming values. Actors are attached to the inputs and the outputs of a dataflow graph. In sense, the actors lie on the boundary of the flow graph but terminate the flow of data as sources and sinks of data, and so are sometimes called terminators.

Data Store: A data store is a passive object within a data flow diagram that stores data for later access. Unlike an actor, a data store does not generate any operations on its own but merely responds to requests to store and access data.

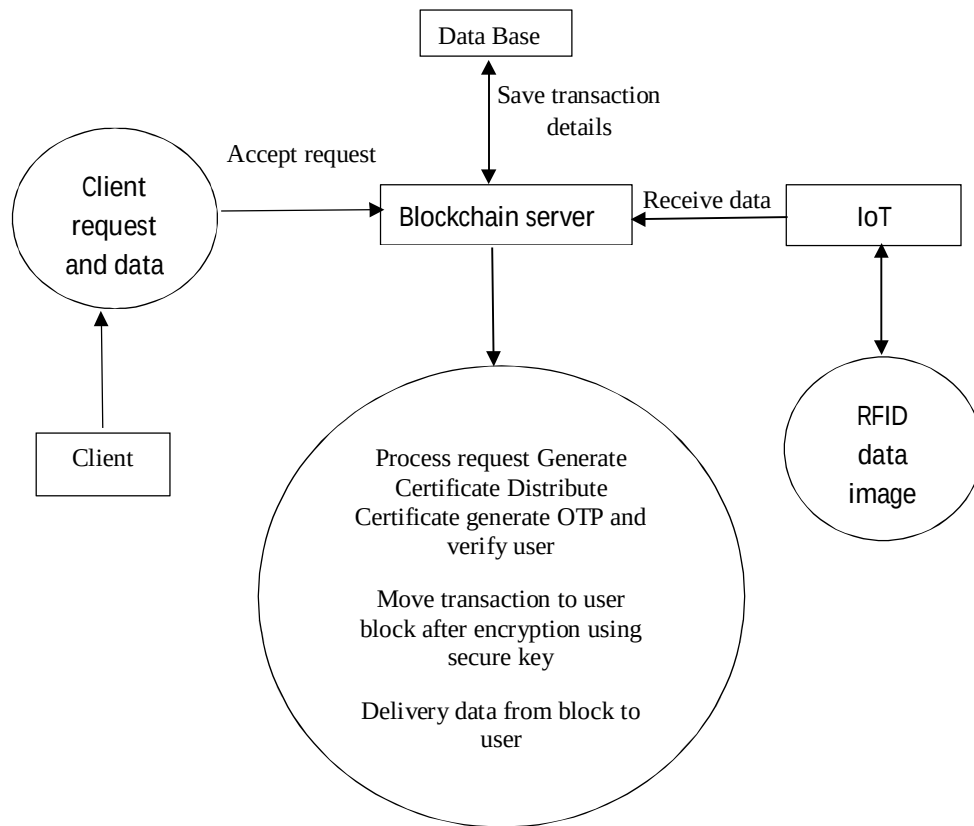


Fig: Data flow diagram for blockchain server

D. Sequence Diagram

The Sequence Diagram models the collaboration of objects based on a time sequence. It shows how the objects interact with others in a particular scenario of a use case. With the advanced visual modeling capability, you can create complex sequence diagram in few clicks. Besides, Visual Paradigm can generate sequence diagram from the flow of events which you have defined in the use case description. The sequence diagram models the collaboration of objects based on a time sequence. It shows how the objects interact with others in a particular scenario of a use case. It depicts the objects and classes involved in the scenario and the sequence of messages exchanged between the objects needed to carry out the functionality of the scenario.

E. Entity Relationship Diagram

Entity-relationship model(ER model) is a data model for describing the data or information aspects of a business domain or its process requirements, in an abstract way that lends itself to ultimately being implemented in a database such as a relational database. The main components of ER models are entities (things) and the relationships that can exist among them, and databases. ER Diagram is a graphical representation of entities and their relationships to each other, typically used in computing in regard to the organization of data within databases or information systems. An entity is a piece of data-an object or concept about which data is stored. A relationship is how the data is shared between entities.

V. RESULT

We introduce a layer of security between user and IOT server. In addition to cryptographic artifact like private key and public key, a further layer of security is introduced by involving certificates. Public key is Used to encrypt the data, and the private key is used to decrypt the data. Once authenticated, the server creates a session for the user. The session may typically last around 30-40 seconds. Within this timeout period, user can communicate with the IoT device and user may control the IoT devices.

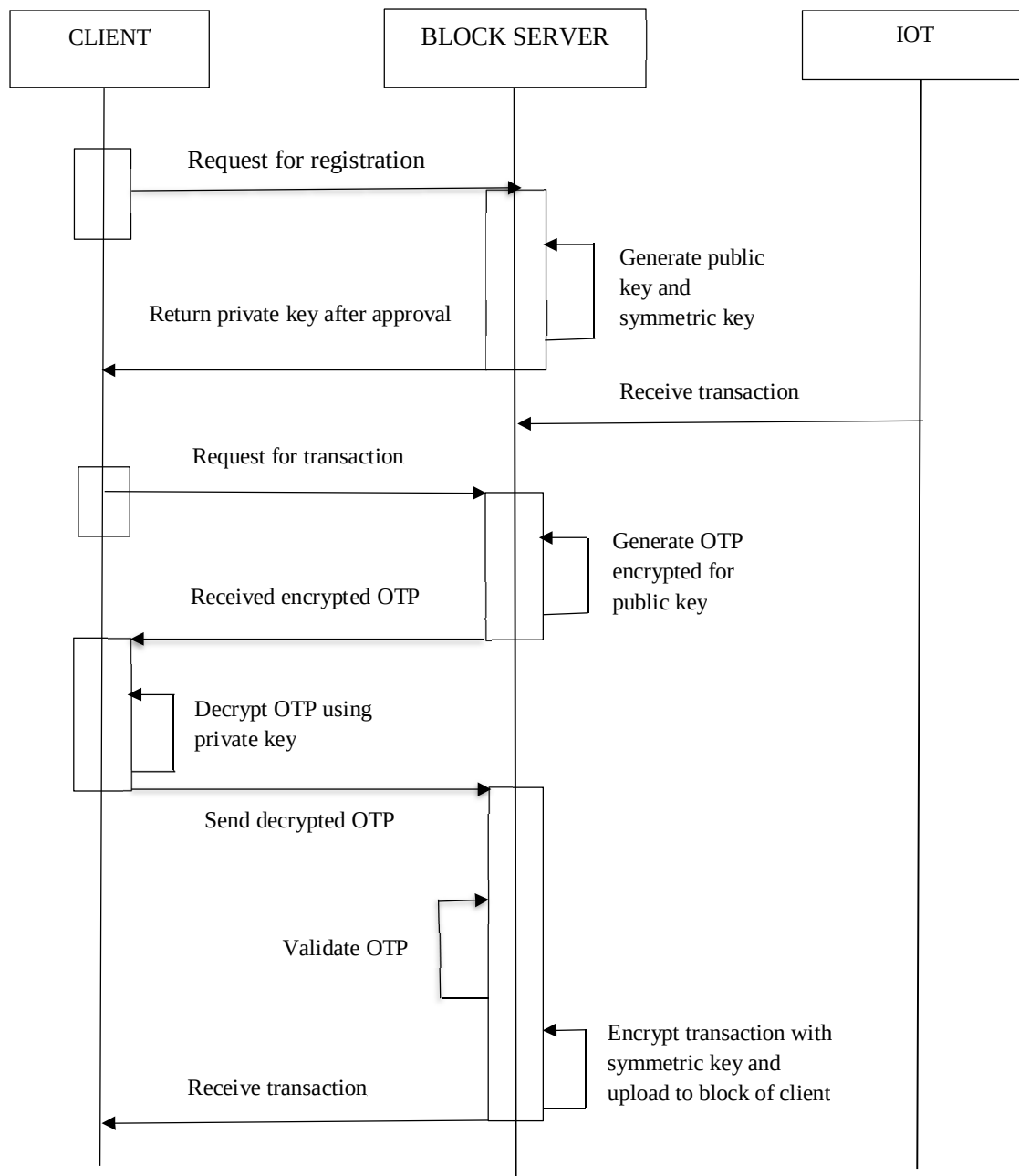


Fig: Sequence diagram

VI. CONCLUSION

The future of blockchain technology itself seems very bright, the reason being that it brings to the table what no other technology brings. The data that is stored on the network can be co-owned by all the parties involved and cannot be modified by any party without the consensus/knowledge of other stakeholders. All this, while maintaining the advantages that distributed, cryptographic system brings. We had cryptographic systems earlier were within the boundaries of an organization. These networks never crossed the boundaries of organization. Blockchain brings all this together to form a holistic system, providing a platform which multiple organizations can use to share data, automate tasks across organizations using smart contracts and much more. All these make blockchain a very powerful technology, leading to a potentially extremely bright future. We can use this any

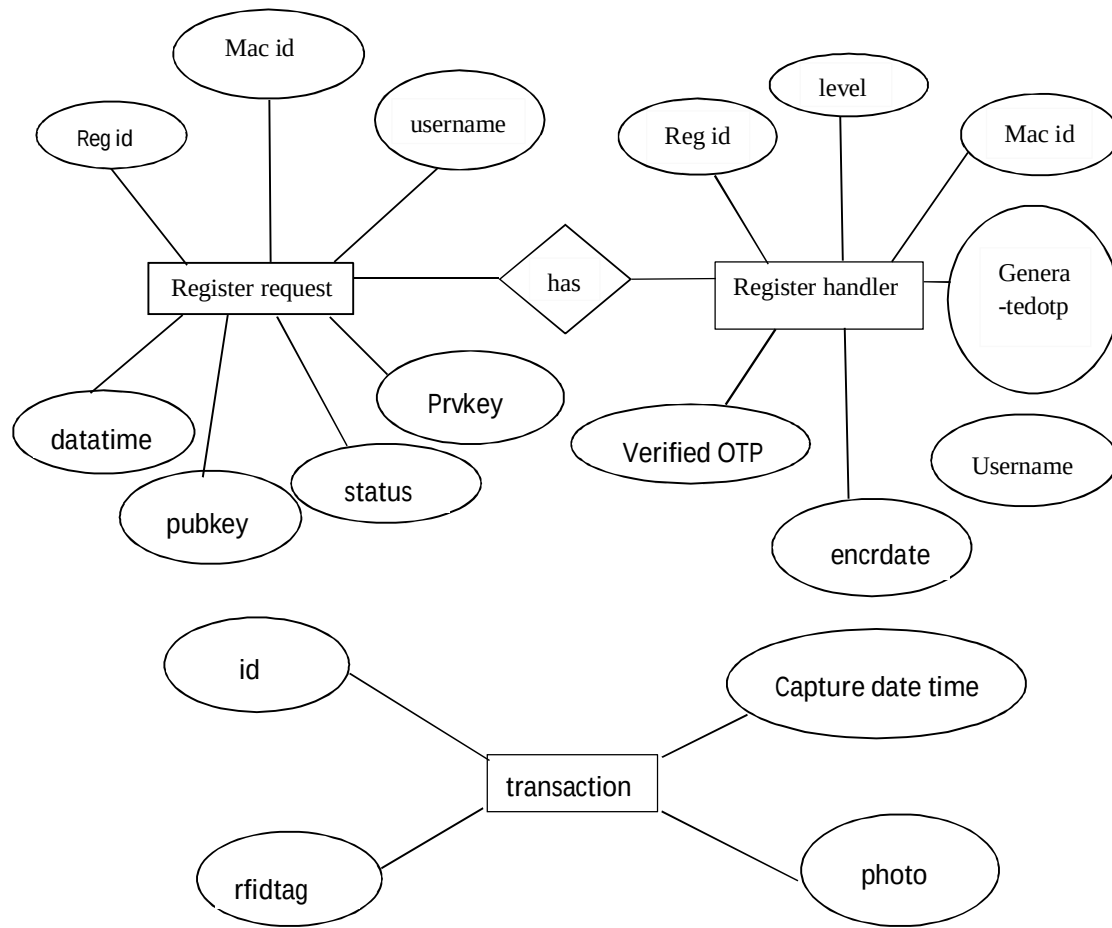


Fig: ER Diagram

domain which has multi parties transacting with each and where there is lack of trust between the parties involved, blockchain can help. Some of the famous domains are F&A, Supply chain management, governance, KYC, Mortgage processing and the list is endless.

REFERENCES

- [1] National Chung Cheng University, Taiwan (February 7-8, 2020) and Chitkara University, India (February 14-15, 2020) Published by Indo Taiwan 2nd International Conference on Computing, Analytics and Networks (IndoTaiwan ICAN 2020).
- [2] Moore, Samuel J., et al. "IoT reliability: a review leading to 5 key research directions." CCF Transactions on Pervasive Computing and Interaction (2020): 1-17.
- [3] Petal. Deepak, Rajiv Ranjan, and Jinjun Chen. "Big Data Stream Security Classification for IoT Applications." (2019).
- [4] Khan. Minhaj Ahmad, and Khaled Salah. "IoT security: Review, blockchain solutions, and open challenges." Future generation computer systems 82 (2018): 395-411.
- [5] Krishnan, K. Navaneeth, et al. "Blockchain based security framework for IoT implementations." 2018 International CET Communication, and Computing (IC4). IEEE, 2018. Conference on Control.
- [6] Guan. Zhitao, et al. "APPA: An anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT." Journal of Network and Computer Applications 125 (2019): 82-92.
- [7] Tharani. Jeyakumar Samantha, Mukunthan Tharmakulasingam, and Vallipuram Muthukkumarasamy. "A blockchain-based database management system. The Knowledge Engineering Review 35 (2020).