MABIDaaS: Mutual Authentication and Financial Transaction Between Mobile Users using Blockchain based ID as a Service

Akshatha B M, Manasa J, Meghana K S, Sonal Salian, Dr. D. Jayaramaiah
Department of Information Science and Engineering
The Oxford College of Engineering, Bengaluru-560068,India

Abstract:In recent times, most of the financial transactions are done through smartphones. Financial transactions contain data of high confidentiality;therefore, security is a main concern in these transactions. Every transaction should be recorded, and this information must be made non-tamperable. Authentication and Authorization of users must be done to check the authenticity of the users to avoid misuse of the data from an intruder. The proposed Mutual Authentication Blockchain based ID as a Service [MABIDaaS] [10] helps to achieve this. Our system uses blockchain technology for storing the transaction details of the user, cloud storage services for access rights, and Trusted Execution Environment [TEE] [11] for a secure execution of the transaction through mobile phones. This paper shows how the proposed system can be used for mutual authentication between two mobile users by using digital signature [3], key set and records the transacted data in the blocks as the data inserted into the blocks cannot be manipulated.

***IndexTerms*–Blockchain, MABIDaaS, Digital Signature, Authentication, Key Generation, Access Rights.**

I. INTRODUCTION

Mobile financial transactions [11] have become a popular mode of transaction. A common man can easily transfer money of any amount to another using merely his phone with a network connection. These kinds of applications require a degree of security, privacy protection and authenticity. The Blockchain based ID as a Service system aims to provide the necessary features.

Blockchain [1] is an open distributed ledger [5] that can record transactions between two parties efficiently. It can also be defined as a continuously growing list of records, known as blocks, which are linked to one another and also secured using cryptography. Transparency and incorruptible nature are the two important properties of Blockchain. Transparency data can be thought as public which is embedded in the network. Any unit of information on Blockchain cannot be manipulated or altered. The Blockchain needs no middleman for digital transactions. The Blockchain eliminates the risks that come with centralized[6] data. Nowadays security problems with the internet is familiar to everyone. Everyone relies on username/password system to protect the identity online. But the Blockchain security methods use encryption technology. The Public and Private keys are the basis for this technology. The public key acts as the users address on the Blockchain.

Trusted Execution Environment [TEE] [14] is introduced to provide a secure environment for exchange of information and financial transactions using private key and with the help of cloud storage. Cloud storage has brought a massive change in the storage industry. Software, platform, and infrastructure can be provided to users as a service from a cloud nowadays. Identity management could be also provided from the cloud to a user. In other words, the user could use an identity and authentication management infrastructure provided from the cloud as a form of IDaaS. [10] It would offer various benefits such as a reduced on-site infrastructure, integrated management with cloud services, and ease use. However, the use of IDaaS means outsourcing critical functions to a third party. All data related to identity and authentication (e.g., user account information, security credentials, etc.) is managed and controlled by the third party without knowing how the data is protected and processed on the cloud. The proposed system MABIDaaS uses cloud to allow the partner to evaluate the access permission rights of each of its registered users. The TEE implemented allows safe and secure transactions between the users without compromising the security using key generation and verification algorithm and transaction between user and partner using private key encryption. In the proposed system the cloud is made more secure and is accessible only by the partner using Secure Hash Algorithm(SHA).

II. EXISTING SYSTEM

Blockchain based ID as a Service is a system which helps in transaction between an individual user and the partner of the BIDaaS provider. The user can transact with the partner without registering himself with the partner if registration with the BIDaaS provider is done. The

BIDaaS provider stores the virtual ID and the public key of the user in the block. A user when requests the partner to its services, the partner checks the integrity of the user by checking if the ID sent by the user matches with the registered ID in the blockchain.
Once the confirmation is done, the partner takes the public key of the user to encrypt any data to be sent to the user using this key. Once the data is received by the user, he uses his private key to decrypt the data to get the original message.
The existing BIDaaS uses the blockchain to store the transaction details and works as an identity and authentication management but lacks in terms of security. Also, there is no constraint on the services permitted to each user which can result in posing as a threat to the financial transaction. This was a matter of concern in the field of finance, therefore there was a demand for a new type of BIDaaS.

Demand for BIDaaS with added security for Authentication

In any transaction, it is very important to validate both the peers identity before making a transaction. Thus, using Blockchain Technology, users can use an Identity and Authentication management infrastructure. This new feature also requires the functionalities of cloud computing. These days we observe that using cloud we can implement different softwares, Platforms, Infrastructures etc. This feature helps to reduce the on-site infrastructure that would be used otherwise. Every single transaction between the same or different users must be validated every time. This decreases the chances of deceit. Thus, it is important to implement BIDaaS so that crucial transactions in Blockchain are verified and protected from a third-party intrusion or viewing the transaction details. The use of Fingerprint Technology and encryption of the transaction details adds that extra edge to this new system and helps in providing extra security.

III. PROPOSED BLOCKCHAIN BASED ID AS A SERVICE- MABIDaaS

In this paper, we provide another version of BIDaaS which provides more security, authenticity and secrecy for more secure financial transactions. We have used the implementation of the Trusted Execution environment, Cloud for Storage and Key Generation for improving the existing system. Figure 1 shows the system architecture of the Proposed System.

A. Components

1) **BIDaaS Provider**: This component's main function is to take the information from the user, store the information in the database and save the user's virtual id and the public key in the blockchain.

2) **Financial Transaction Centre**: This is the unit which provides any transactional facilities to the users. In our paper the FTC is a bank whose users are the transactors.
The financial transaction centre gives the permission of the transaction of each user.

3) **Users**: Users are the end users and the people who and the transactions. Each user will have a unique virtual id and generates a public key pair in their devices for the encryption and decryption of their transactions.

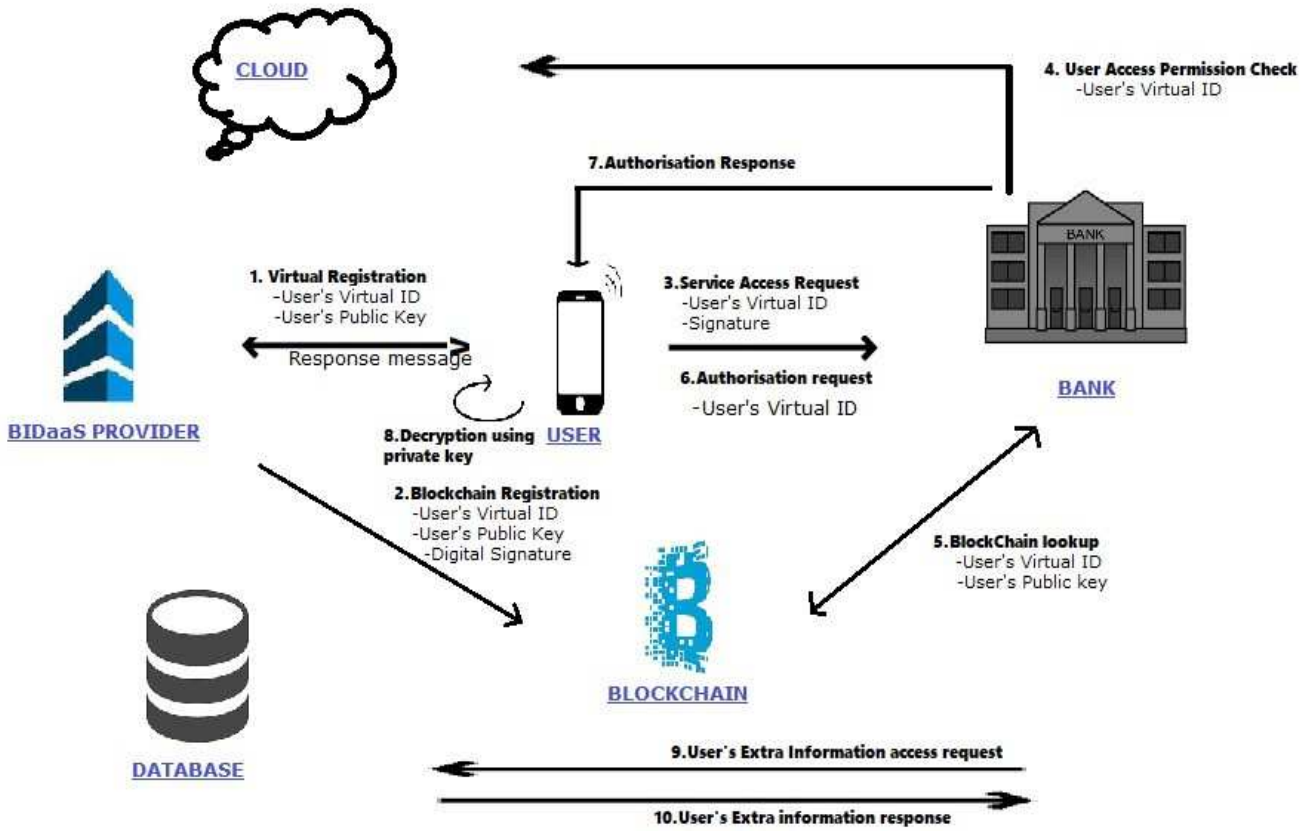

Fig 1: System Architecture of MABIDaaS

B. Procedures

1) **Registration**: The process starts with the user registering with the BIDaaS provider which acts as a third-party verifier in the later stages. The user gives in the his/her account number, name, email id, phone number and the password. The user generates a public key pair in his/her device and stores the private key in his device and sends the public key to the provider. The BIDaaS provider inserts the user' s virtual ID and the user generated public key into the block. The fingerprint of the user is taken during the registration process.

2) **Login**: The user signs into his/her account by using the virtual id and password. The user has toauthenticate by giving his/her fingerprint which is compared with the fingerprint taken during the registration process. The user sends an access request to the BIDaaS provider which generates an OTP and send it to the registered mobile number. This acts like another layer of authentication.

3) **Add amount**: A user can transfer some amount from his bank account to the secret account which is used for the transaction, this amount detail is added into the block and the new variations on the amount is reflected in the block.

4) **Transaction**: Once the user is successfully logged into their account, they get a list of activities that they can do. The user has to select another registered user with whom he/she wants to do any transaction. The Financial Transaction Centre [FTC] authorizes the transaction bychecking with the cloud if the two users can proceed with the transactions.

For the transaction:

Key-Generation: One of the user generates a set of keys and encrypts it using the public key of the other user and sends it to them. The other user decrypts it using their private key

Single transaction: The user can transfer the amount details to the other user using the first key from the key set as a mode to encrypt the data. The receiver user can use the first key of the key set to decrypt the details and store it in the block.

The two communicating users can prove their authenticity by their digital signatures[3]. After the authenticity check, the users can generate a set of key and pass it to the other. Each key is used and discarded after respective transaction.

A user can login only through the given handset which holds his/her fingerprint and the transaction is run in the secure part of the OS called the Trusted Execution Environment.

DFD LEVEL 0

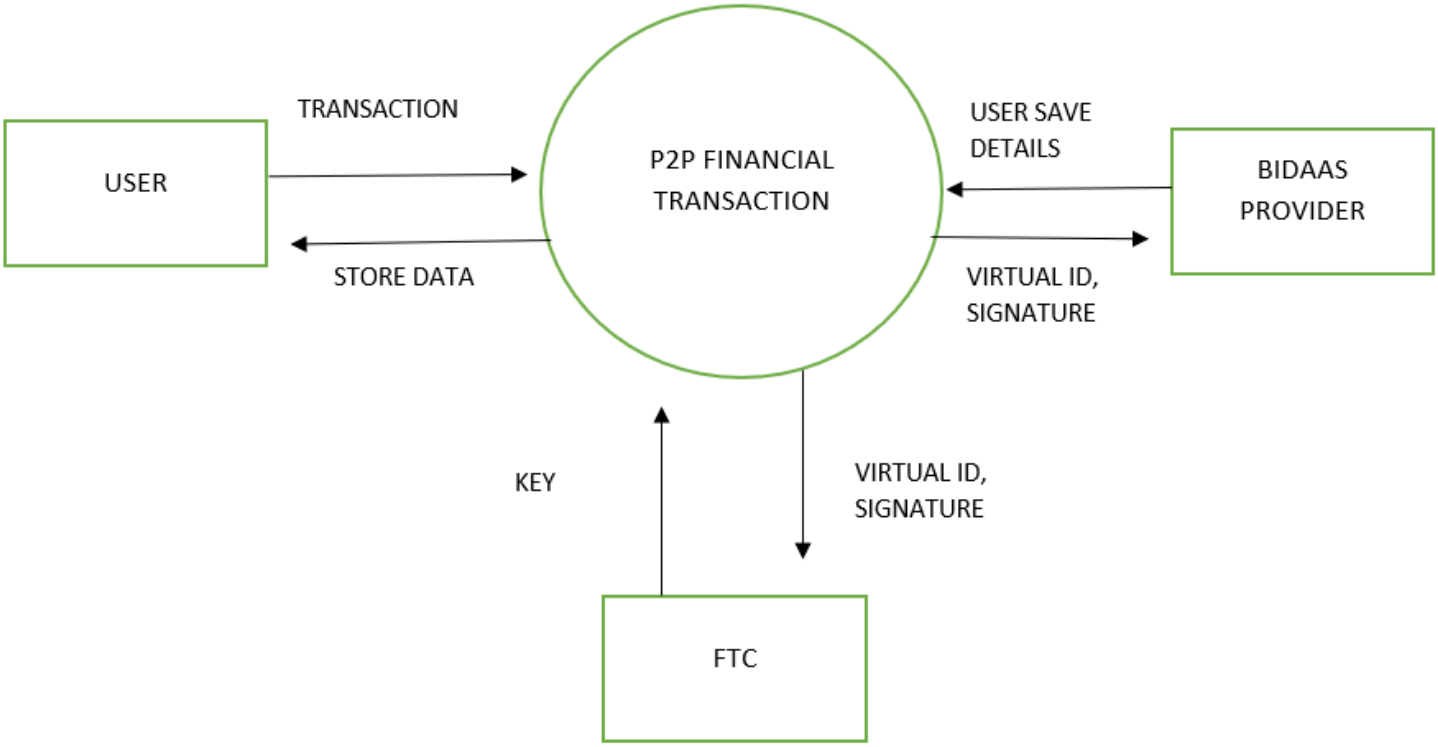

Figure 2: Data Flow Diagram of Level 0

DFD LEVEL 1

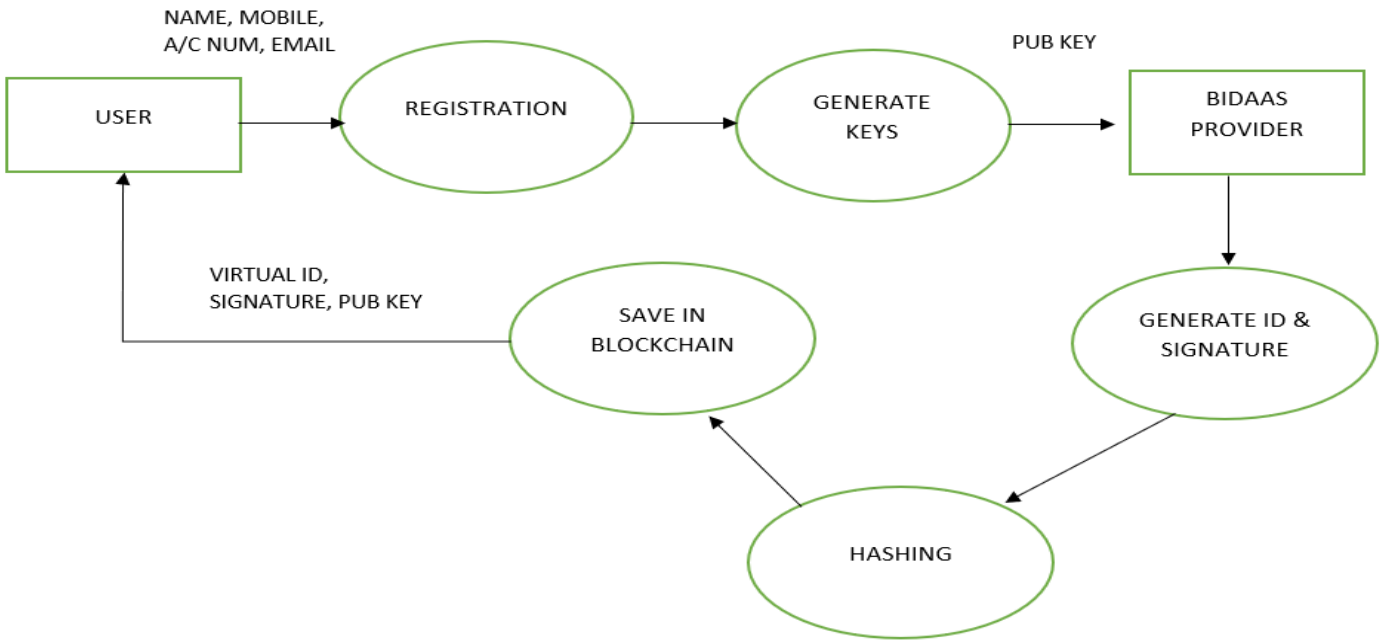

Figure 3: Data Flow Diagram of Level 1

DFD LEVEL 2

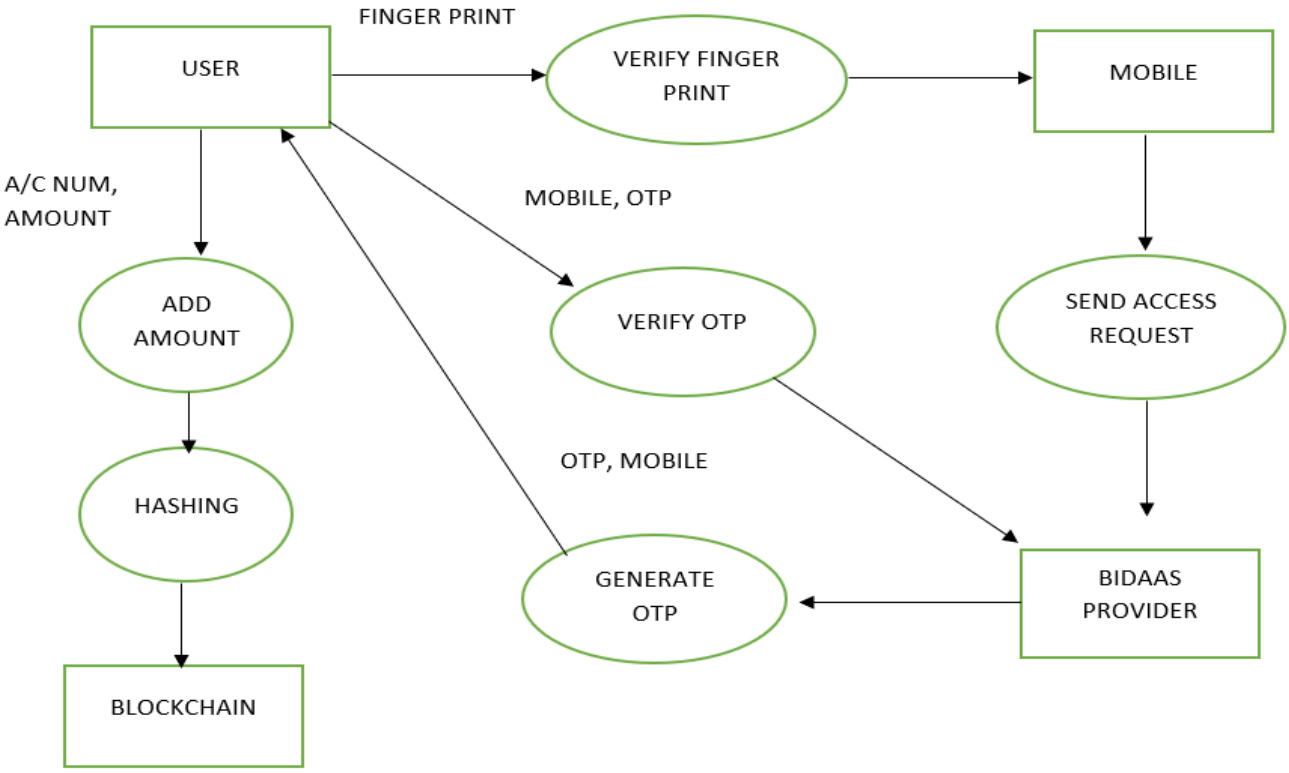

Figure 4: Data Flow Diagram of Level 2

DFD LEVEL 3

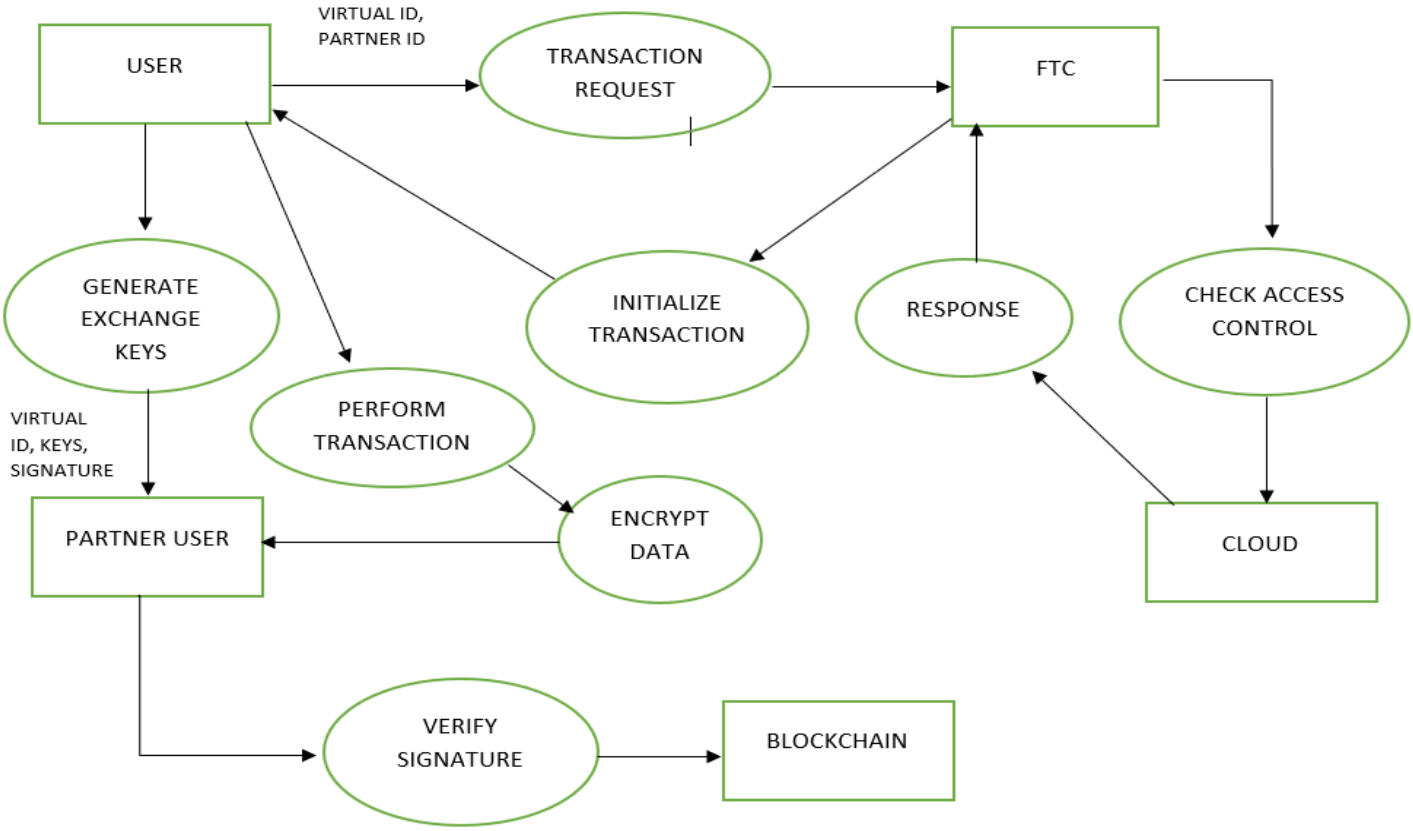

Figure 5: Data Flow Diagram of Level 3

DFD LEVEL 4

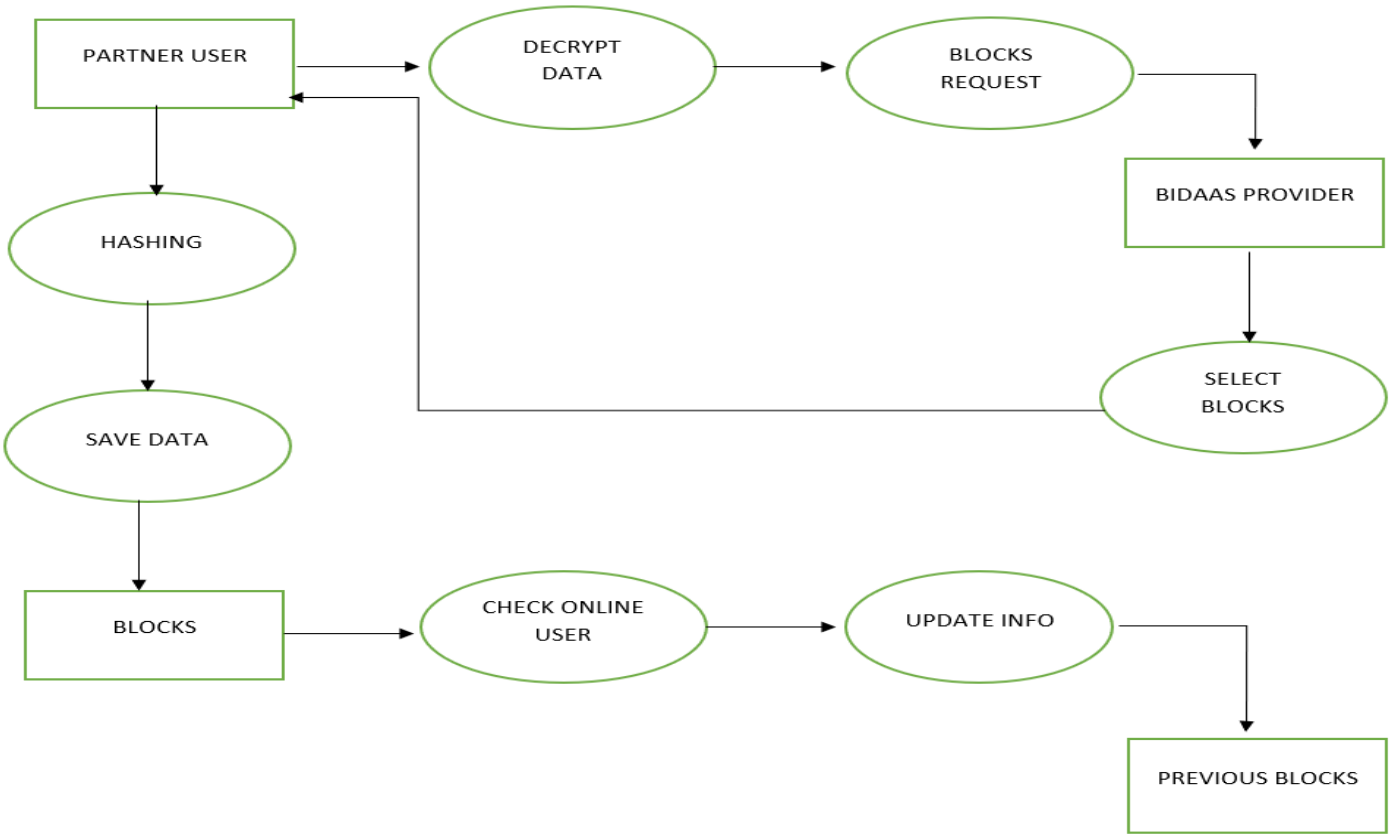

Figure 6: Data Flow Diagram of Level 4

C. Example

Let there be 2 users named X and Y respectively. Both of them register with the BIDaaS and their virtual ID and Public key is stored in the Blockchain. Now X wants to send Rs 500 to Y. X transfers Rs 1000 from his bank account to the account which handles the transaction. This amount is stored in the BIDaaS. X requests communication with Y from the Financial Transaction Centre [FTC]. The FTC checks for the access right permissions of both users. If permission is granted, the two users prove their authenticity with digital signature and X generates 10 keys and encrypts it using Y's public key and sends it to Y. Y decrypts the key set using his private key. A then encrypts Rs 500 using the first key of the key sets and sends it to Y. This transaction is stored in the blockchain. Y uses the same key from the key set and decrypts the message and updates its wallet amount which is appending this transaction into its device's block. Both X and Y then delete the key used fr this transaction from the key set. 9 more transactions can be done after which one of the user has to generate another set of keys and send to the other.

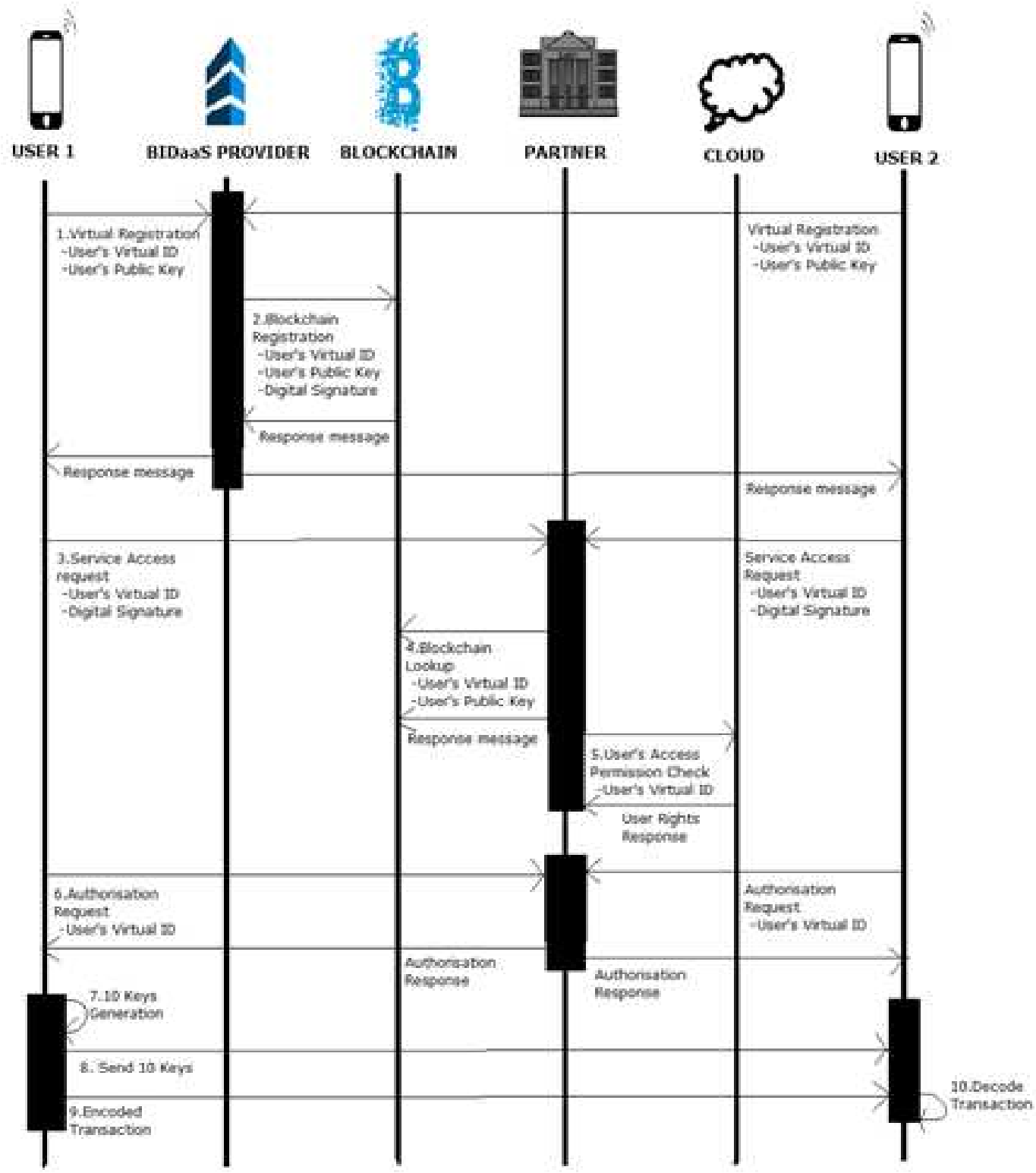

fig 2: Sequence diagram for a single transaction between two user

IV. FEATURES OF THE SYSTEM

A. Consensus Algorithm

The blockchain used here is a private blockchain. The miners are selected based on the computational power i.e., based on the timing, beginning time and end time is noted and the miners are selected. Each miner selected gets an amount as a reward.

B. Consortium Blockchain

The blockchain used here is a private blockchain which is not owned by the BIDaaS provider. The blockchain is a distributed ledger and is operated by consortium members. The user account information is accessed from the BIDaaS provider when needed, the user information is not shared among all consortium members present in the blockchain.

C. Provided User Information

Extra user information is provided to the BIDaaS provider and Financial Transaction Center (FTC). This is not only for storage purpose but also provide better privacy, avoiding the misuse of the information provided.

D. Use of virtual IDs

Every user is assigned by a virtual ID. This virtual ID assigned to the user is unique. The user can use the virtual ID if it is already registered in the blockchain.

E. Private Key of a User

Private key is a secret key which is stored in the user mobile. Each user has a different private key stored in an electronic device. Key generation material and other sensitive information is stored in the trusted execution environment.

F. Benefits to the BIDaaS Provider

The BIDaaS provider creates new sources of revenue by providing an identity and authentication management solution as well as providing existing user information to its partners.

G. Benefits to the User

A better security is provided to the user by various levels of verification. Digital signature is included as well as key set exchange during transaction provides better security. The user details are registered in blockchain and it can be accessed when necessary and the details in the blockchain cannot be tampered hence provides a better security for transactions.

H. Benefits to the Financial Transaction Centre

Financial transaction center (FTC) which is the partner gets service request from the user. FTC looks up the blockchain for details and checks the permission rights for accessing the services, of the user from the cloud. The presence of the FTC extends its level in authorization by providing the access permission rights of the user.

Table 1: Comparison between BIDaaS and MABIDaaS

Properties	BIDaaS	MABIDaaS
Access rights	The BIDaaS system does not facilitate the use of cloud to store the access permission rights of its users.	The MABIDaaS system facilitates the use of cloud to store the user access rights.
Security	The security level in existing system is compromised due to the lack of sufficient authentication and verification protocols applied between partner-user and user-user communication.	More Security is achieved in MABIDaaS system using private key encryption algorithm.
Communication	Communication here takes place only between the partner and the user using wireless communication medium.	In MABIDaaS system, Communication occurs between partner-user and between user-user using wireless communication medium. This added feature helps to broaden the horizon of transactions that can occur in the environment.
Authentication Protocols	One layer of Authentication Protocol exists between the BIDaaS provider, Partner and the registered users.	Multiple Layers of Authentication protocol exists between the different components of the system, paving way for a more secure system than the existing system.

To summarize with the comparison of the existing system BIDaaS and the proposed system MABIDaaS, the MABIDaaS provides more secure features compared to the BIDaaS. Firstly, MABIDaaS allows the partner to selectively authorize users for whom access rights are granted. These rights are stored in the cloud which can be accessed only by the partner i.e., the Financial Transaction Centre. Secondly, each transaction is encrypted using different keys available only to the two communicating user whereas in the BIDaaS, encryption is done using only the user's public key. Thirdly, in BIDaaS, Communication was done only between the user and the partner whereas in MABIDaaS, communication between two users is allowed. Lastly, another authentication is through the key set, as only the user having the key set same as the sender can decrypt the message.

V. CONCLUSION

MA-Blockchain based ID as a service focuses on the authentication and authorization. In this paper we have discussed an example which shows financial transactions between the mobile users using MABIDaaS. Security is provided by adding authentication in the form of key generation set and authorization through permission rights given to the user. Financial transaction centre checks the access rights of the user in the cloud.The act of providing the access rights to the user by storing it in the cloud has further improved the authorization measures of the system. Keys are generated and exchanged, and each key is used as a mode for encryption and decryption for each transaction respectively. The proposed system provides a secure transaction between the users without the partner having any knowledge of the financial transactions. Trusted Execution Environment is used in MABIDaaS which provides a secure area for the mobile application and the data loaded inside in terms to integrity and confidentiality.

The proposed MABIDaaS has some room for improvement. The expansion of the area of network in which the transaction can take place between the user can smoothen the usage of the system.

REFERENCES

[1] How the Blockchain Revolution Will Reshape the Consumer Electronics Industry. Jong-Hyouk Lee and Marc Pilkington,IEEE Consumer Electronics Magazine,Volume 6,Issue 3,July 2017.

[2] Ethereum: A Secure Decentralized Generalized Transaction Ledger. DR.GavinWood,CTO Ethereum Project.

[3] A Digital Signature Based On A Conventional Encryption Function. Ralph C. Merkle, 1987.

[4] Making Byzantine Fault Tolerant Systems Tolerate Byzantine Faults. Allen Clement and Edmund Wong, Published in:Proceeding NSDI'09 Proceedings of the 6th USENIX symposium on Networked systems design and implementation, Boston, Massachusetts April 22 - 24, 2009.

[5] Architecture of the Hyperledger Blockchain Fabric. Christian Cachin, IBM Research-Zurich, 2009.

[6]Is Bitcoin a Decentralized Currency? Arthur Gervais, Ghassan O. Karame, SrdjanCapkun and VedranCapkun, IEEE Publication,Issue No. 03 - May-June (2014 vol. 12).

[7]Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin. Ghassan O. Karame, Elli Androulaki and SrdjanCapkun, Published in: Proceeding CCS '12 Proceedings of the 2012 ACM conference on Computer and communications security, Raleigh, North Carolina, USA October 16 - 18, 2012.

[8]Information Propagation in the Bitcoin Network. Christian Decker and Roger Wattenhofer, Published in: Peer-to-Peer Computing (P2P), 2013 IEEE Thirteenth International Conference on 9-11 Sept. 2013.

[9]An Analysis of Anonymity in the Bitcoin System. Fergal Reid and Martin Harrigan, Volume 2, 7 May 2012.

10]BIDaaS: Blockchain Based ID as a Service. Jong-Hyouk Lee, published in IEEE,volume 20, 2017.

11]An Ecosystem of Trusted Execution environment of Smartphones- A potentially bumpy road, IEEE 2017.

12] Provably secure and lightweight identity-based authenticated data sharing protocol for cyber-physical cloud environment.
ArijitKarati, Ruhul Amin, S.K HafizulIslam , Kim-Kwang Raymond Choo, Published in: IEEE, 08 May 2018

13]Secure cloud storage and Quick Keyword based Retrieval system.Songfeng Lu, Abdulruhuman I Ahmed Abomakhelb, Published in :IEEE 2017

14] Open-TEE—An Open virtual trusted execution environment. Brian McGillion, TanelDettenborn, Thomas Nyman, N Asokan, IEEE 2015

15]Automated Partioning of Android applications for Trusted execution environment, Konstantin Rubinov,LuciaRosculete,Tulika Mitra, AbhikRoychoudhury, IEEE 2016