I. J. Computer Network and Information Security, **2024, 6, 69-82**
Published Online on December 8, 2024 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2024.06.06

GDAR: A Secure Authentication for Dapp Interoperability in Blockchain

Surekha Thota*
REVA University/School of Computer Science and Engineering, Bengaluru, 560064, India
E-mail: surekhaswarup@gmail.com
ORCID iD: https://orcid.org/ 0000-0003-2872-2366
*Corresponding author

Shantala Devi Patil
REVA University/School of Computer Science and Engineering, Bengaluru, 560064, India
E-mail: shantaladevi.patil@reva.edu.in
ORCID iD: https://orcid.org/0000-0002-9157-758X

Gopal Krishna Shyam
Presidency University/Department of Computer Science and Engineering, Bengaluru, 560064, India
E-mail: gopalshyambabu@gmail.com
ORCID iD: https://orcid.org/0000-0001-5562-5794

Bhanu Prasad
Florida A&M University/Department of Computer and Information Sciences, Tallahassee, FL 32307, USA
E-mail: bhanu.prasad@famu.edu
ORCID iD: https://orcid.org/0000-0002-3585-655X

Received: 07 May 2023; Revised: 26 July 2023; Accepted: 18 October 2023; Published: 08 December 2024

Abstract: Enterprises are adopting blockchain technology to build a server-less and trust-less system by assuring immutability and are contributing to blockchain research, innovation, and implementation. This led to the genesis of various decentralized blockchain platforms and applications that are unconnected with each other. Interoperability between these siloed blockchains is a must to reach its full potential. To facilitate mass adoption, technology should have the ability to transact between various decentralized applications (dapps) on the same chain, integrate with existing systems, and initiate transactions on other networks. In our research, we propose a secured authentication mechanism that enables various decentralized applications on the same chain to interact with each other using a global dapp authentication registry (GDAR). We carried out an in-depth performance evaluation and conclude that our proposed mechanism is an operative authentication solution for dapp interoperability.

Index Terms: Blockchain, Interoperability, Decentralized Applications, Authentication Mechanism, Credit Bureau.

1. Introduction

1.1. Importance of Interoperability in Enterprises

Digitization not only improves the productivity and efficiency of the business by capturing the data, but also facilitates easy integration of business systems. Every organization has its own mission-driven core business goals. Organizations strive to focus on their line of interest rather than building a complete end-to-end solution. Outsourcing is a business process that delegates the business activity to a third-party system to solve time, manpower, and financial constraints [1]. Smart businesses outsource the business functionalities that are not aligned with their business goals and interoperate with third parties to consume the services produced. Let us consider a couple of scenarios that demand business to obtain services from others.

Scenario 1: The Government regulations and anti-money laundering laws in several countries impose the financial institutions to verify the documents that demonstrate the identity, address proofs, and legality of the customers [2]. Two constraints that arise in this situation are i) additional overhead for the banks to verify and validate the proofs submitted by the customer as it is not the banks' main line of business. Any non-compliance reported will charge an ample amount on the banks [3]. ii) if a customer applies for loan in two banks, then both the banks need to validate and verify his/her identity, thus involving a lot of redundant work. To stay focused, smart financial institutions integrate with the third-party identity verification service provider, which is known as "Know Your Customer" (KYC) [4].

Scenario 2: With an increase in fraud rate and by considering the safety of its own employees and organizations, many companies conduct background verification of the shortlisted candidates during job offerings. According to the UK Trends and Best Practices Report, 78% of companies have agreed to conduct a pre-employment background check [5]. This check can either be carried out in-house or consult a third-party verification team who does a thorough verification of the proof submitted by the new joiners. In practice, some businesses need to collaborate and interoperate with other relevant businesses to attain mutual benefit.

1.2. Issues with Existing Banking, Financial Services and Insurance (BFSI)

The existing BFSI industry not only use centralized servers but also integrates with various legacy systems that work on different technologies, standards, and protocols. Cybersecurity is of paramount importance in BFSI. Even though BFSI invests and implements several algorithms to provide confidentiality, integrity, authentication, privacy, and non-repudiation of information, it encounters many attacks [6]. Financial firms are likely to get attacked 300 times more than other industries [7]. Even though BFSI invested a lot of money, time, and effort in addressing these non-functional security requirements, it still struggles with the following open issues:

(1) Nontransparent data across systems - Each party involved in business maintains its bookkeeping separately, which is closed from the public. Reconciliation between these businesses is conducted at regular intervals [8].

(2) Data tampering - Traditional ledgers are vulnerable to tampering by a malicious record-keeper [8].

(3) Single point of failure - Use of centralized servers and database may result in a single point of failure [8, 9].

(4) Lack of trust among stakeholders - Trust is a crucial factor in the financial sector. It can be built by refraining the banks from behaving opportunistically. Existing system ledgers are closed from the public; therefore, this process cannot guarantee trust among various stakeholders [10].

(5) High transaction fee - With an increase in the number of intermediaries between the customer and the organization, the transaction fee increases [8, 10].

(6) Information Asymmetry - Central authorities create an asymmetry in data and may try to overuse the power to generate money [11, 12]. Credit bureaus are an example of revenue generation because of information asymmetry.

(7) Longer Settlement time - Settlement [trade/transaction settlement] takes more time, as it does not take place at real-time [13, 14].

Blockchain [2, 15] is considered a breakthrough in technology as it addresses the above issues. Blockchain provides an alternative and improvised solution in various domains and sub-domains [16, 17, 18]. Blockchain based Rain Drop Service verification scheme and Fingerprint Biometric verification is proposed to prevent cyber-crimes in banking transactions [19]. In the following subsection, we present an overview of blockchain along with the issues it can resolve and the new challenges that open to implement it for real cases.

1.3. Overview of Blockchain and How it Addresses the Above Issues

Blockchain is a distributed append-only verifiable ledger [20]. Blockchain-enabled BFSI ensures that data is transparent (addressing issue 1 above), immutable (Write-Once, Read-Many) (addressing issue 2 above), and provides confidence that "WHAT I SEE IS WHAT YOU SEE" (addressing issue 3 above) [21]. It removes information asymmetry by ensuring that the data is publicly open and distributed to all stakeholders of the network (addressing issue 4 and 5 above) [14]. In Permissioned Blockchains, the transactional fee is usually low (addressing issue 6 above). Settlement of transactions is carried out by miners, facilitating instant reconciliation (addressing issue 7 above).

Ethereum blockchain uses smart contracts to create a digital agreement between the buyers and sellers [21]. Deployed smart contracts are trackable and irreversible. Different decentralized applications (dapps) are created for different business requirements [22, 23]. Dapps may or may not use blockchain and are built on peer-to-peer decentralized network [15, 24, 25]. In this research, we consider dapps that interact with the blockchain and manages the state of all actors in the network as shown in Fig.1. The front-end of a dapp is very similar to that of centralized applications, and the backend represents business logic powered by smart contract. Decentralized applications build an immutable, transparent, and information symmetric system, but they are not mature enough on these aspects as centralized applications. Hence, research is being carried out in version controlling, bug fixing, coupling multiple dapps together, achieving scalability and so on. In this research we focus on achieving interoperability between various dapps.

The chain of events carried out during our research are discussed as below. In the Literature Review section, we analyze several challenges while achieving interoperability between various dapps and by credit bureaus. In the Methodology section, we propose a secure authentication mechanism that enables decentralized applications on the same chain to interact with each other using a global dapp authentication registry (GDAR). In the Results section, we present the implementation of the proposed model for achieving secure interoperability between financial institutions and credit bureaus, then evaluated the experimental results.

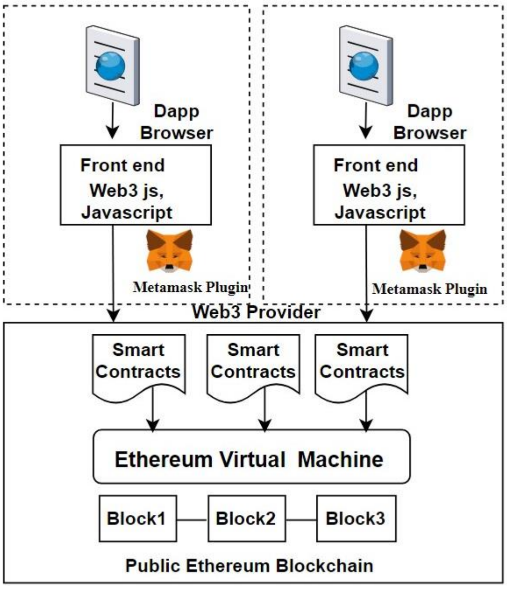


Fig.1. Dapp interaction with ethereum

2. Literature Review

The literature review is carried out in two directions. First, we discuss the problems in blockchain while achieving interoperability and, second, concerning the credit bureau system which is our case study.

2.1. Literature in Blockchain Technology while Achieving Interoperability

Blockchain has the potential to build better-connected businesses [26]. Motivations behind using blockchain for development have been summarized in [27-29]. It removes friction between various stake holders and tries to perform settlement in real time [10]. Blockchain based authentication and access control technique is proposed for secure data sharing between cloud owners and users [30-32]. To address the privacy issues associated with cloud storage, a blockchain based private storage system is proposed [33]. Blockchain has introduced new problems that act as hindrance while applying it for real world scenarios.

- Blockchains work in Silos - Unlike Cloud-based centralized systems, initial generations of blockchain operates in silos, therefore, impedes seamless transactions between multiple blockchain platforms [34]. To overcome this, various interoperable blockchain solutions have emerged and they use different Interoperability schemes and Finality consensus. A comparative study of some of these interoperable blockchain products and schemes are discussed [35-38].
- Privacy of data - According to Article 5 of European Union (EU) General Data Protection Regulation (GDPR) the seven key data protection principles are lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability [40]. Blockchain is a public ledger and restricts the privacy of transactions [40, 41].

What businesses need from an enterprise blockchain platform is the ability of multiple applications to run across a common layer of identity, consensus, and governance. Integration can happen at the application level, system level, business level, or enterprise level [34]. The security and privacy requirements while achieving interoperability are adaptable trust management, fine-grained access control and privacy preserving encryption [42]. In our research, we focus on application-level integration, specifically on dapp integration. Dapps should have a mutually collaborative relationship such that various applications should be able to share the data between them. If an application has to send or receive data from another, they must strictly follow some semantics, so that the data sent by one is understood by others. There are several advantages of dapp when compared to traditional applications [43]. “State of the dapps” project maintains the list of decentralized applications built on various blockchain platforms [44]. The owner of a dapp can submit the details of their dapp to the “State of the dapps” project. This project maintains the name of the dapp, description, author, status, category, URL of the dapp along with its smart contract address on the main network. This enables the users to download the app and make the required transactions. By clicking the link of the smart contract address, the user can view all the transactions that took place on the app. The limitation of this project is that it stores information about the details of a single dapp, however, it does not have the details of how an app can interact with others.

2.2. Survey on Our Case Study - Credit Bureaus

When a customer applies for a loan or credit card, his/her credit risk assessment is estimated before the required services are approved. Several parameters like payment history, credit utilization, length of credit history, credit types, inquiries, professional background, collateral, education, family background and social media profile are considered for credit score calculation [45]. Risk arises to the financial institution when a customer exhibits inability to repay as agreed. When the volume of defaulters increases, the current reserve of the financial institution depletes and may eventually lead to losses. The responsibility of the offering financial institution is to evaluate and predict the repayment capability of the customer. Credit bureaus are the private bodies that demonstrate a role in maintaining and providing credit scores to the customers [46, 47]. This generated credit score acts as one of the key considerations by the financial institution in making the final judgment on the application of the customer. Equifax [48], Experian [49], and TransUnion [50] are some of the examples of credit bureaus.

The following are some of the open challenges faced by the centralized credit bureaus that lead to the pavement of new requirements.

- The Survival of Credit bureau systems is mainly due to the asymmetry of information. Credit bureaus typically gather data of all the customers from various creditors and then calculate the creditworthiness of each customer based on that customer's repayment history. Thus, it led to a non-transparent information model.

The solution is to replace the centralized credit bureau system with an open and transparent blockchain system that can avoid information asymmetry. Colendi community aims to assess the credit score using a distributed approach [51, 52]. It tries to replace the centralized credit bureau systems with decentralized ones, thus eliminating the drawback of information asymmetry. In addition to the repayment history, the Colendi algorithm processes both the past and real-time data to provide a reliable credit score. As the credit score generated by Colendi has no boundaries, it is valid globally as is deployed on the blockchain network.

- Credit bureaus typically gather the information of all customers from various creditors and then calculate the creditworthiness based on their repayment history. As this information is not updated directly by the customers, it may lead to data inaccuracy.

As per the Credit Information Companies Regulation Act in India, information regarding every retail loan and the customer's repayment details should be reported to the credit bureaus [53]. However, the nonfinancial data of the customers also has an impact on credit repayment capabilities. The life of a customer can change drastically because of an unexpected event. This event could be the death of the primary salary contributor in the household, loss of employment, disability due to an accident, and health issues, etc. Hence the customer should be given an option to update his non-financial data to the credit bureau with the submission of appropriate documents.

- Customer does not have data ownership (Privacy Control): Any organization can access the credit bureau score of a customer regardless of the customer's interest. The customer should have a provision to choose and authorize the requests and decide whether he/she permits the organization to access this data or not. It does not seek any consent from the customer. According to the Protection of Personal Information Act (POPI Act) [54], the customer should confirm before a business can access his/her credit report. It depends on the corresponding Nation's Credit Act. To protect the privacy of customer's data, we take consent from the customer while filling the application for credit check processing.

Guppy addresses this by using blockchain wallet feature [55]. Each time consumer's data is accessed, the consumer gets paid, and customer's wallet shows the complete list of transactions along with the public address of financial institution that have accessed the data, including the portion of data it has accessed, and the access date and timestamp.

- Identity theft: Privacy of personal data is compromised as the information is under the control of a centralized database. A massive data breach at Equifax in 2017 compromised the personal information, including Social Security numbers of 147 million consumers [48]. On July 22, 2019, as part of a court settlement, Equifax agreed to distribute around 500 million dollars to those affected.

3. Methodology

BFSI gives utmost importance to information security. It focuses on all the security features like confidentiality, integrity, authentication, non-repudiation, and denial of service. It uses various techniques like multi-factor authentication, encryption, and real-time masking of fields to guarantee network and information security. Multi-factor authentication and encryption are the biggest obstacles for hackers [56]. Despite implementing all these techniques, traditional banking systems still suffer from hacking.

3.1. Challenges and Proposed Solutions in Achieving Interoperability

Blockchain is considered a definitive solution for some of the challenges faced by traditional centralized banking systems. However, it pops out some of the new challenges like interoperability, scalability, and standardization. Our research mainly focuses on interoperability. Five different challenges, along with some proposed solution(s), to achieve interoperability between two decentralized applications, are provided next.

A. First Challenge - Secure Interoperability between Two Dapps

Business objectives demand a collaborative relationship among various business partners, regulators, and third parties. This research mainly focuses on achieving interoperability between dapps of different businesses that complement each other. Decentralized applications should be collaborative and capable of authenticating each other. A blockchain-based dapp is accessed by Business to Consumer (B2C) or Business to Business (B2B). However, in B2C, interoperability may not be applicable as users can directly access the dapp, whereas B2B requires a secure way of communication between two dapps.

Proposed solution to address the first challenge: To address the above-stated interoperability issue, in B2B, we need to identify whether a dapp has required permissions to access another dapp or not. For simplicity, we represent the dapp providing the service as server dapp or dapp initiator, and the dapp requesting the information as client dapp. The server dapp proposes a one-time offline registration process for client dapps to sign Memorandum of Secure Interoperability (MoSI) between two parties and generates MoSI_ID to enable secure transactions between these two dapps. GDAR is a smart contract that validates the permission of client dapps to access the server. In our proposed design, we maintain three different fields in GDAR for achieving interoperability between two decentralized applications, shown in Table 1.

Table 1. GDAR

Server_Unique_ID	Client_Unique_ID	Encrypted_MoSI_ID

On completion of MoSI process, server dapp inserts records to GDAR ledger by encrypting MoSI_ID using the Public key of the server (Pu_s) as shown in eqn. (1).

$$E_{GDAR} = E\left[MoSI\_ID\right]_{Pus} \tag{1}$$

All client dapp requests must include E_{Client} to enable secure transmission of MoSI_ID on the network. MoSI_ID is first encrypted with the private key of the client (Pr_c) and then with the public key of the server (Pu_s) as in eqn. (2).

$$E_{Client} = E\left[E\left[MoSI\_ID\right]_{Prc}\right]_{Pus} \tag{2}$$

On receiving the request, the server dapp decrypts it using the private key of server (Pr_s) and then the public key of Client (Pu_c) as in eqn. (3).

$$D_{Client} = D\left[D\left[MoSI\_ID\right]_{Puc}\right]_{Prs} \tag{3}$$

Server dapp then invokes GDAR bypassing the Server Unique ID and Client Unique ID, and then fetches the corresponding E_{GDAR}. E_{GDAR} is decrypted using private key of the server as in eqn. (4).

$$D_{GDAR} = D\left[E_{GDAR}\right]_{Prs} \tag{4}$$

The request is considered valid only when D_{GDAR} is same as $D_{Client.}$

B. Second Challenge - Identification and Authentication of Trusted Entities

BFSI transacts only with trusted customers. Customers submit KYC to banks, so are trusted by the banks, whereas Bitcoin and Ethereum blockchains are pseudo-anonymous and use a public network. It opens the following challenges: i) how do we authenticate and restrict the users of an application on a public network and ii) how to identify and allow who can access what functionalities of a dapp.

Proposed solution to address the second challenge: The user logs on to the blockchain with a combination of a public and private key. A user can create multiple such accounts. A solution to uniquely identify and authenticate the trusted users on a public network is to choose a consortium blockchain with permission to only trusted entities. But how to identify and verify whether the users have access to a particular module in a dapp? In our design, we propose a two-factor authentication. The first level of authentication is carried out at the blockchain level by using the combination of public and private key. At the second level, we maintain a GDAR, which identifies and controls the user access rights of a dapp along with their permissible functional access. In our proposed design, we extend the GDAR by adding access rights at the module level. Access rights specify whether the client is an “endorser”, who is directly involved in the transaction or a “reviewer”, who can only view the transaction. Revised GDAR is shown in Table 2.

Table 2. Revised GDAR

Server_Unique_ID	Client_Unique_ID	Encrypted_MoSI_ID	Access_Rights_for_Modules

C. Third Challenge - Protecting Identity Theft

The incident with Equifax in 2017 had proven that there is a compromise in protecting the privacy of customer’s personal information when the data is under the control of a centralized system [48]. Preserving the privacy of a dapp deployed on the blockchain is challenging as its key capability is to provide openness and transparency to all the users.

Proposed solution to address the third challenge: Preserving the privacy of the customer is of utmost importance. Blockchain is an open and transparent system. To prevent identity theft, one must avoid disclosing personal information on a public network. The following solutions may be applicable to preserve the privacy of the customer.

Design choice 1- Use of consortium blockchain instead of public blockchain: Unlike a public blockchain, consortium blockchain restricts access to limited nodes with similar interests [57]. It ensures privacy to a certain extent, but in some scenarios, it is challenging when other nodes are business competitors.

Design choice 2- Usage of private transactions: Transactions are made private while using confidential data.

Design choice 3- Hashing technique to mask data: Masking is a technique of concealing the data with modified content. Masking fields try to strike a balance between data transparency and protecting customer data. Masking the required data helps to achieve confidentiality by not disclosing the information on public networks.

Design choice 4- Consent from customer: According to the POPI Act, the customer has complete authority to provide his/her approval before sharing his personal information [54].

D. Fourth Challenge - Standardized Data Format

Standardization is needed to achieve a meaningful data exchange between various dapps. However, proposing a global standard data format is not possible as the data formats usually depend on the domain and the business functionality. The challenge is to propose a standard data format while achieving interoperability between dapps.

Proposed solution to address the fourth challenge: An interface is developed between the client and server by accepting the request and response data formats of the server. Sharing this request and response formats between various businesses is carried out during the MoSI phase specified in the proposed solution to address the first challenge explained above.

E. Fifth Challenge - Compliance

The data stored on the blockchain is immutable and permanent, and the deployed smart contract cannot be modified [58]. However, most of the applications are updated frequently because of bugs, change requests, and compliance regulations. For example, all businesses should adhere to the rules provided by their corresponding accrediting organizations. The following are some of the regulatory compliance systems [59].

- PCI-DSS and GLBA in the financial industry
- HACCP for the food and beverage industry
- Joint Commission and HIPAA in healthcare

The challenge here is how to accommodate and operate consistently with the changing regulations to avoid penalties for law violations [60].

Proposed solution to address the fifth challenge: The functional expert should identify and decide which part of the data should be on-chain and what goes off-chain. The data that needs transparency and immutability is placed on the blockchain, and the data that needs frequent changes should go off-chain. A model-view-controller (MVC) approach is suggested to implement the compliance regulations in blockchain [61, 62].

3.2. Case Study: Interoperability between Credit Decision Dapp and Credit Bureau Dapp

This section describes how the above discussed proposed solutions are applied and implemented to the case study that simulates the interoperability between Credit Decision System (CDS) and the Credit Bureau system (CBS). CDS processes the loan/card application submitted by the client and decides whether to accept or reject that application. CBS provides credit score for a given customer. In our case study, CBS and CDS are decentralized applications that were built on Ethereum. Fig.2. depicts that the CBS dapp (dapp initiator/server) deployed on Ethereum blockchain is accessed by all financial institutions.

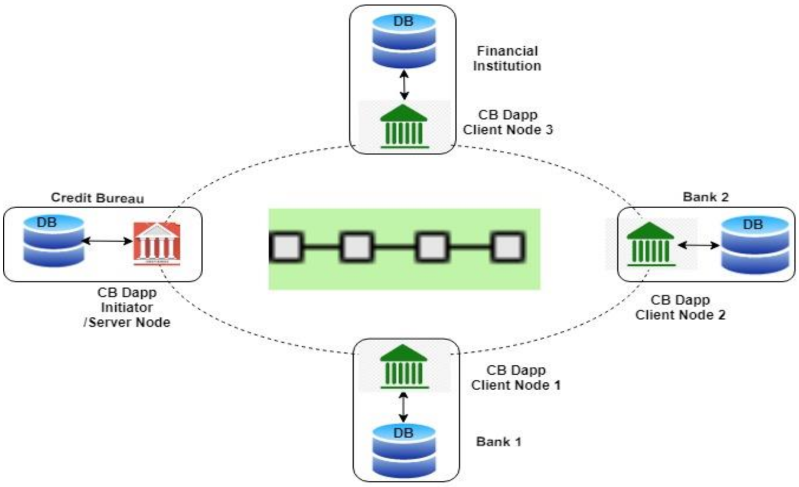


Fig.2. Credit Bureau dapp accessed by all banks, money lenders, and other financial institutions

In general, financial institutions such as banks, credit card issuers, and money lenders are the clients for credit bureaus. In our case study, we consider financial institution (or bank) as a client that seeks credit score from the credit bureau dapp. Fig.3. depicts various functionalities carried out by credit bureau and financial institutions. In this research, we focus on ‘Disseminate Credit Score’ and ‘Credit Decision management’ functionalities.

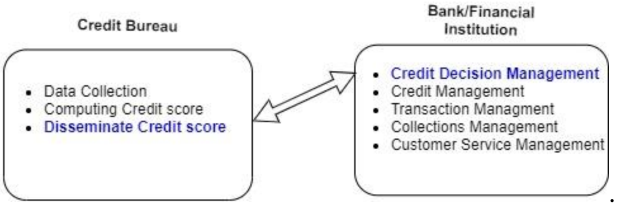


Fig.3. Interaction between credit bureau and financial institution

When a customer applies for a loan, the financial institution performs prechecks for rejecting the blacklisted and fraud applications. The CDS of that financial institution processes the valid applications and sends a request to check the credit score of the customer to CBS. CBS responds to the CDS with a credit score. CDS will decide whether to approve or reject the application by considering the credit score and other parameters like VIP applicant, number of dependents the customer has, salary, etc. Financial institute forwards the decision taken by CDS to the customer. Fig.4. depicts the sequence of steps involved in retrieving the credit score of a customer.

The following part of this section explains how the proposed solutions are applied for this case study.

Addressing challenges 1 and 2: The GDAR smart contract had been implemented to maintain the Server ID, Client ID, encrypted MoSI_ID and allowed functionalities. As part of one-time registration process, the Credit Bureau and Financial institute signs the memorandum of secure interoperability (MoSI) and agrees upon the MoSI_ID. The CBS then updates the GDAR with Server_ID, Client_ID, encrypted MoSI_ID, and allowed functionalities.

Addressing challenge 3: To ensure privacy, certain fields (such as some characters in unique Id) in the client request can be masked. On successful authentication, the credit bureau forwards the request to the customer to seek his/her authorization for sharing the credit score to the financial institution.

Addressing challenge 4: As part of MoSI (one-time registration process), the server shares the request and response formats with the client. In addition to the functional information, the request format should include Server ID, Client ID, encrypted MoSI_ID, and allowed functionalities to comply with the proposed solutions of first two challenges.

Addressing challenge 5: The pattern followed here is MVC. Model is the MoSI procedure that finalizes the request and response data format to store the necessary information. View is the front-end of CDS. Controller is the CBS and GDAR that provides authenticated interoperability between dapps. The algorithm for achieving secure interoperability between CDS and CBS using GDAR is described in Algorithm 1. The complete request-response cycle in building this secure dapp authentication mechanism is depicted in Fig.5.

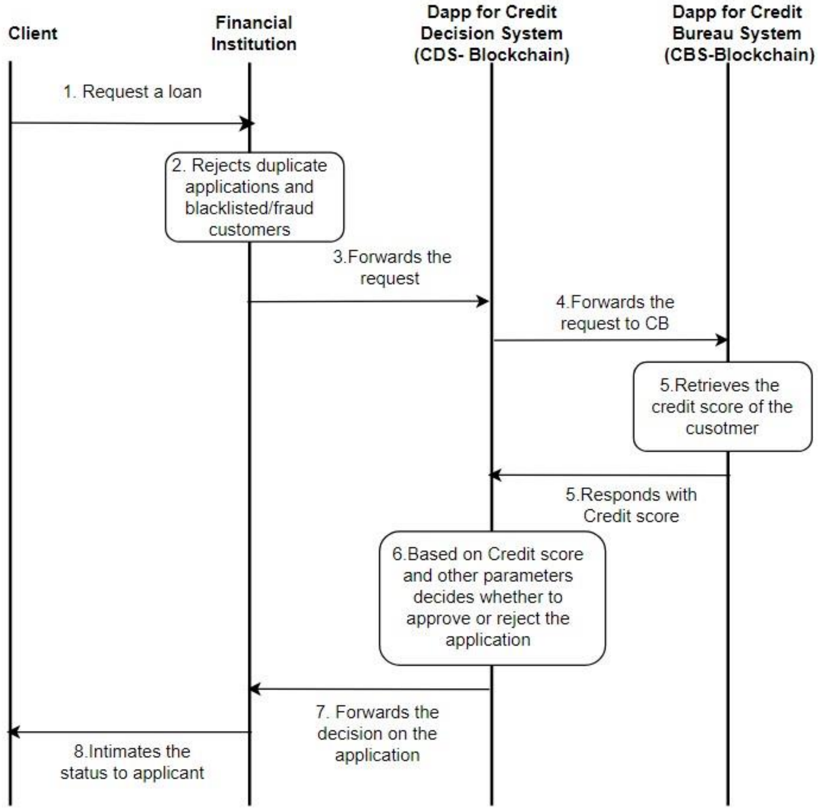

Client
Financial Institution
Dapp for Credit Decision System (CDS- Blockchain)
Dapp for Credit Bureau System (CBS-Blockchain)
1. Request a loan
2. Rejects duplicate applications and blacklisted/fraud customers
3.Forwards the request
4.Forwards the request to CB
5.Retrieves the credit score of the cusotmer
5.Responds with Credit score
6.Based on Credit score and other parameters decides whether to approve or reject the application
7. Forwards the decision on the application
8.Intimates the status to applicant

Fig.4. Interoperability between CDS and CBS dapp to retrieve credit score for valid customers

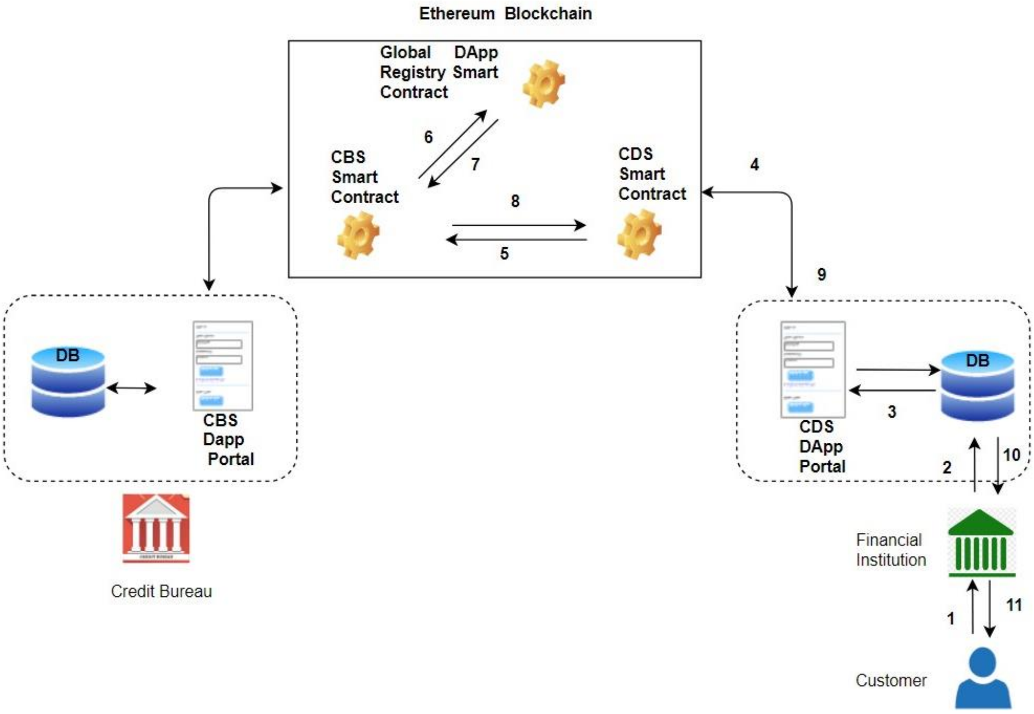


Fig.5. Sequence of steps followed to depict interoperability between CDS, CBS and GDAR

Algorithm 1: Sequence of steps involved in achieving secure interoperability between CDS and CBS using GDAR

- Customer applies for a loan to financial institution.
- The financial institution performs pre-checks and removes blacklisted and fraud applications.

- The valid applications are forwarded to CDS dapp Portal.
- CDS dapp invokes CDS smart contract.
- CDS smart contract forwards the request along with server ID, client ID, encrypted MoSI_ID ($E_{Client} = E[E[MoSI\_ID]_{Prc}]_{Pus}$) and function name to CBS smart contract
- CBS decrypts E_{Client} ($D_{Client} = D[D[MoSI\_ID]_{Puc}]_{Prs}$) and invokes the GDAR by passing server ID and client ID
- GDAR fetches the corresponding encrypted MoSI_ID ($E_{GDAR} = E[MoSI\_ID]_{Pus}$) and access rights that are stored in GDAR after MoSI Phase and then responds to CBS.
- CBS now decrypts E_{GDAR} ($D_{GDAR} = D[E_{GDAR}]_{Prs}$) and validates if D_{GDAR} is same as D_{Client} to check the authenticity of client. For valid customers, CBS retrieves the credit score and forwards it to CDS smart contract.
- CDS smart contract now forwards the creditscore to CDS dapp
- Based on credit score and other parameters (such as VIP customer, outstanding assets, number of dependents the customer has), CDS decides whether to approve or reject the application.
- Financial institution forwards the decision taken by CDS dapp to the applicant.

4. Results

In this section, we present the implementation details of our proposed model by depicting secure interoperability between CDS and CBS using GDAR for the case study. The specifications of the implementation setup are Intel(R) Core(TM) i5-1035G1CPU@1.00 GHz, 8 GB RAM, 64-bit operating system, and X64-based processor. For the deployment, we have used Remix IDE, MetaMask Wallet, Ganache as a private Ethereum Blockchain and Sepolia as a public test Ethereum network.

In Ethereum, the gas consumed for contract creation or function execution depends on the complexity, computational requirements, and storage allocation. Each operation within the function consumes certain amount of gas, and the cumulative gas cost of all operations determines the total gas consumed. Tools like Remix IDE or Truffle can help to estimate the gas cost for deploying the contract or function execution. Specify the gas limit for the transaction deployment. If the gas consumed exceeds the gas limit, the transaction will fail due to an out-of-gas error.

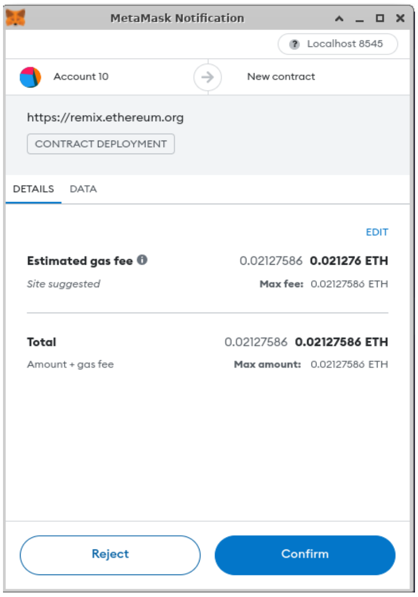
Simulation Setup

Three different smart contracts CDS (Loan Application), CBS (Credit Bureau), and GDAR are developed using remix IDE. These contracts are first deployed on the private blockchain using Ganache. Sample Contract deployment on Ganache using MetaMask is depicted in Fig.6.

To capture the amount of gas used in live settings, the same is deployed on the Sepolia test public network. We tested the proposed model for the following three different scenarios:

Case i) We record the amount of gas consumed for contract creation and execution of various functions in Table 3. Fig.7a represents the gas consumed for both Sepolia and Ganache. These statistics show that contract creation takes more gas compared to actual transactions or function calls.

Case ii) We perform a self-comparative study by increasing the number of records from 1 to 10, 20, and 30 on both Ganache and Sepolia networks. Fig.7b and Fig.7c depict the test results of the Ganache and Sepolia. We notice that the consumption of gas increases as we increase the number of records in both Ganache and Sepolia.



Localhost 8545

Account 10 → New contract

https://remix.ethereum.org

CONTRACT DEPLOYMENT

Estimated gas fee 0.02127586 **0.021276 ETH**

Site suggested **Max fee:** 0.02127586 ETH

Total 0.02127586 **0.02127586 ETH**

Amount + gas fee **Max amount:** 0.02127586 ETH

Fig.6. Contract deployment on ganache using metamask

Case iii) We record the minimum and maximum gas consumed for invoking the getcreditscore() function. Fig.7d depicts the gas consumed for fetching the first and last record of getcreditscore() for a varying number of records. We observe that i) the gas consumed is constant while retrieving the first record and ii) gas increases proportionally to the increase in the number of records.

Our proposed solution is an add-on feature that provides additional security using GDAR. The dapp registry consumes 1775092 gas in Ganache and 1462404 in Sepolia for contract creation, a one-time process. It also consumes 180632 and 204972 in Ganache and Sepolia for searching a single record. This additional gas consumption provides an add-on authentication mechanism for providing secured interoperability between smart contracts.

Table 3. Gas consumed by ganache and sepolia

SmartContract	Function	Gas_Used_Ganache	Gas_Used_Sepolia
dapp_global_registry	Contract_Creation	1775092	1462404
dapp_global_registry	addvalDetails()	243814	238574
dapp_global_registry	getValidation()	1137261	133821
Credit_Bureau(CBS)	Contract_Creation	1839971	1491111
Credit_Bureau(CBS)	addCredit_Details()	90875	92211
Credit_Bureau(CBS)	getscore()	137677	140271
Credit_Bureau(CBS)	setaddr()	43232	42584
Loan_Application(CDS)	Contract_Creation	1994840	1647172
Loan_Application(CDS)	SetApplicant()	287520	282624
Loan_Application(CDS)	Creditreq()	180617	156954
Loan_Application(CDS)	setaddr()	43182	42534

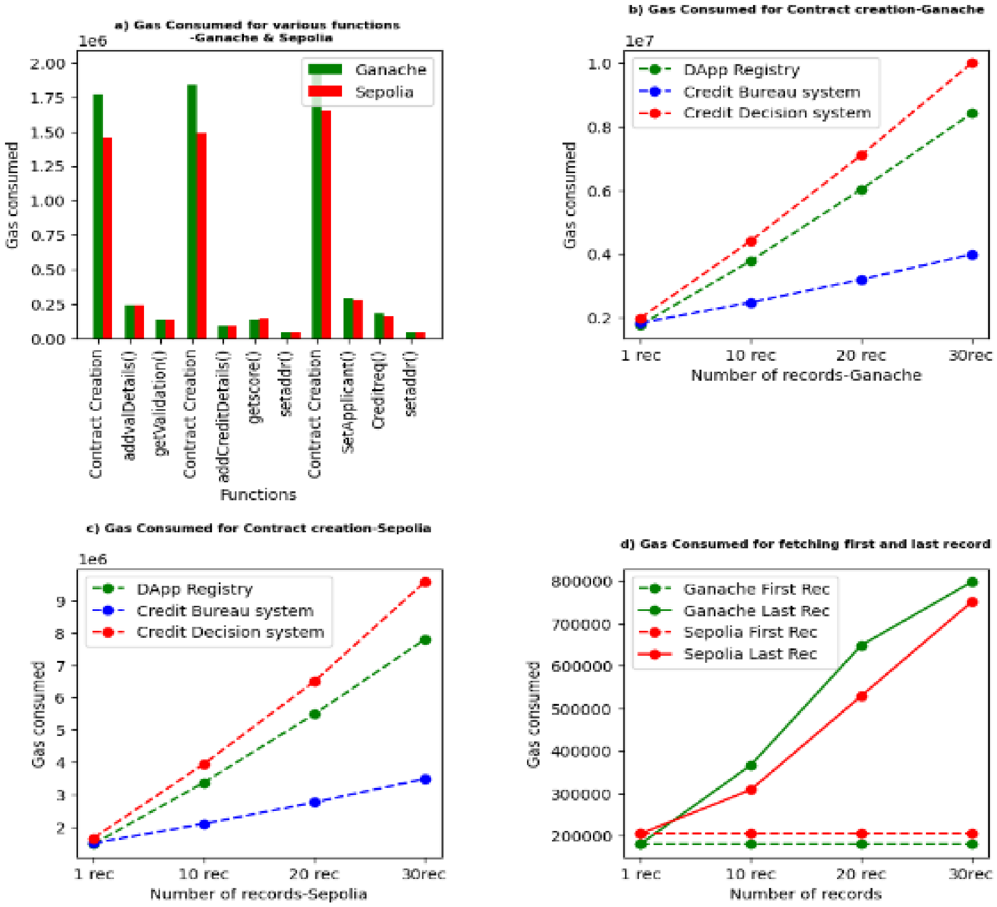


Fig.7. Gas consumption for different scenarios

5. Conclusions

Blockchain is a decentralized public system and anyone, who knows a contract address and ABI (Application Binary Interface), can invoke its functions. This access mechanism compromises the privacy of applications on the blockchain. BFSI is highly prone to hacking and implements many security tools. Hence, there should be a control on who can access which smart contract.

In this research, we proposed a method wherein two decentralized applications residing on the same blockchain platform can securely interoperate with each other. This research implements a GDAR to ensure secure interoperability. It validates and controls who can access what functionalities of the dapp. Ethereum provides authentication by a pair of public and private keys whereas our proposed design GDAR proposes a multi-factor authentication at both blockchain and dapp level. In addition, GDAR allows peer to peer transactions with MVC architecture. This study has successfully developed and deployed credit bureau and banking smart contracts using GDAR that demonstrates enhanced trust and security in dapp interoperability.

GDAR authentication can be implemented to achieve the following features in a multiple decentralized application. i) Secure Data Sharing: GDAR ensures that only authorized users can initiate cross-dapp transactions, preventing unauthorized access and tampering sensitive information. ii) Secure Smart Contract Communication: GDAR ensures that only authorized smart contracts can invoke specific functions or modify contract states, protecting against unauthorized or malicious actions. iii) Access Control: Enables fine-grained control over the actions and data that different dapps can access or modify when interacting with each other. iv) Compliance and Regulatory Requirements: GDAR helps dapps to comply with regulatory requirements, such as KYC and Anti-Money Laundering (AML) rules in a secured manner.

In the future, i) we bring more flexibility to the one-time registration process (MoSI) by making this online processing, ii) we enhance GDAR to make it a repository of all dapps that are implemented on all blockchain platforms, iii) we investigate on strong identity management tools that minimize the data storage on blockchain, and iv) we refine the study by deploying the authentication mechanism on various blockchain platforms.

Acknowledgement

The authors would like to acknowledge the support provided by REVA University.

References

[1] Alexandra Twin, Margaret James, and Pete Rathburn, “Outsourcing: How It Works in Business, With Examples,” Investopedia, Jun. 18, 2022. https://www.investopedia.com/terms/o/outsourcing.asp (accessed Feb. 12, 2023).

[2] Martin and L. Taylor, “Exclusion and inclusion in identification: regulation, displacement and data justice,” Inf Technol Dev, vol. 27, no. 1, pp. 50–66, 2021, doi: 10.1080/02681102.2020.1811943.

[3] Toby Tiala, “The Case for Outsourcing Your KYC,” EQ, Nov. 17, 2017. https://equiniti.com/uk/news-and-views/eq-views/the-case-for-outsourcing-your-kyc/ (accessed Feb. 12, 2023).

[4] N. Lalitha and D. Soujanya, “Financial sector Innovations: Empowering Microfinance through the application of KYC Blockchain technology,” in *International Conference on Digitization (ICD), Sharjah, United Arab Emirates*, 2019, pp. 237–243.

[5] Sterling, “Benefits of Outsourcing Background Checks to a Third-Party Provider,” *Sterling*, Sep. 05, 2018. https://www.sterlingcheck.co.uk/blog/2018/09/benefits-outsourcing-background-checks/ (accessed Feb. 12, 2023).

[6] K. AL-Dosari, N. Fetais, and M. Kucukvar, “Artificial Intelligence and Cyber Defense System for Banking Industry: A Qualitative Study of AI Applications and Challenges,” *Cybern Syst*, pp. 1–29, Aug. 2022, doi: 10.1080/01969722.2022.2112539.

[7] Bricata, “10 Statistics that Summarize the State of Cybersecurity in Financial Services,” *security Boulevard*, Nov. 12, 2019. https://securityboulevard.com/2019/11/10-statistics-that-summarize-the-state-of-cybersecurity-in-financial-services/ (accessed Feb. 12, 2023).

[8] Adabi Joseph and Markus Brunnermeier, “Blockchain Economics,” 2022. doi: 10.3386/w25407.

[9] A. N. Gohar, S. A. Abdelmawgoud, and M. S. Farhan, “A Patient-Centric Healthcare Framework Reference Architecture for Better Semantic Interoperability Based on Blockchain, Cloud, and IoT,” *IEEE Access*, vol. 10, pp. 92137–92157, 2022, doi: 10.1109/ACCESS.2022.3202902.

[10] W. Viriyasitavat, L. Da Xu, Z. Bi, and A. Sapsomboon, “Blockchain-based business process management (BPM) framework for service composition in industry 4.0,” *J Intell Manuf*, vol. 31, no. 7, pp. 1737–1748, 2020, doi: 10.1007/s10845-018-1422-y.

[11] Evan Tarver, Michael J Boyle, and Suzanne kvilhaug, “How Financial Markets Exhibit Asymmetric Information,” *Investopedia*, Jul. 28, 2022. https://www.investopedia.com/ask/answers/042915/how-do-financial-market-exhibit-asymmetric-information.asp (accessed Feb. 12, 2023).

[12] R. Wang, Z. Lin, and H. Luo, “Blockchain, bank credit and SME financing,” *Qual Quant*, vol. 53, no. 3, pp. 1127–1140, May 2019, doi: 10.1007/s11135-018-0806-6.

[13] “How blockchain could disrupt banking,” *Research Brief, CBinsights*, Oct. 18, 2022. https://www.cbinsights.com/research/blockchain-disrupting-banking/ (accessed Feb. 12, 2023).

[14] John McLean, “Banking on blockchain: charting the progress of distributed ledger technology in financial services,” *A Finextra white paper produced in associate with IBM*, Jan. 2016.

[15] Narayan Prusty, *Blockchain for Enterprise*, 1st ed. Packt Publishing, 2018. Accessed: Feb. 12, 2023. [Online]. Available: https://www.perlego.com/book/823710/blockchain-for-enterprise-build-scalable-blockchain-applications-with-privacy-interoperability-and-permissioned-features-pdf

[16] J. R. Varma, “Blockchain in Finance,” *Vikalpa*, vol. 44, no. 1, pp. 1–11, Mar. 2019, doi: 10.1177/0256090919839897.

[17] M. Javaid, A. Haleem, R. Pratap Singh, S. Khan, and R. Suman, “Blockchain technology applications for Industry 4.0: A literature-based review,” *Blockchain: Research and Applications*, vol. 2, no. 4. Elsevier Ltd, Dec. 01, 2021. doi: 10.1016/j.bcra.2021.100027

[18] Showkat, S., & Qureshi, S. (2023). Securing the Internet of Things Through Blockchain Approach: Security Architectures, Consensus Algorithms, Enabling Technologies, Open Issues, and Research Directions. International Journal of Computing and Digital Systems, 13(1), 97-129.

[19] C. Gomathi and K. Jayasri, “Rain Drop Service and Biometric Verification Based Blockchain Technology for Securing the Bank Transactions from Cyber Crimes Using Weighted Fair Blockchain (WFB) Algorithm,” *Cybern Syst*, 2022, doi: 10.1080/01969722.2022.2103229.

[20] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System.” [Online]. Available: www.bitcoin.org

[21] Richard Brown, “The interoperability challenge will make or break enterprise blockchain platforms,” *Medium*, 2018. https://medium.com/corda/the-interoperability-challenge-will-make-or-break-enterprise-blockchain-platforms-4016518e333d (accessed Feb. 15, 2023).

[22] Daniel Davis Wood, “ETHEREUM: A Secure Decentralised Generalised Transaction Ledger,” 2014. Accessed: Feb. 12, 2023. [Online]. Available: https://ethereum.github.io/yellowpaper/paper.pdf

[23] Y. Pang, “A New Consensus Protocol for Blockchain Interoperability Architecture,” *IEEE Access*, vol. 8, pp. 153719–153730, 2020, doi: 10.1109/ACCESS.2020.3017549.

[24] Roberto Infante, *Building Ethereum Dapps*. Shelter Island, NY : Manning Publications, 2019.

[25] David Johnston, Sam Onat Yilmaz, Jeremy Kandah, and Nikos Bentenitis, “The General Theory of Decen-. tralized Applications, DApps,” 2014, Accessed: Feb. 12, 2023. [Online]. Available: http://cryptochainuni.com/wp-content/uploads/The-General-Theory-of-Decentralized-Applications-DApps.pdf

[26] Raihana Syahirah Abdullah, Faizal M.A., "Block Chain: Cryptographic Method in Fourth Industrial Revolution", International Journal of Computer Network and Information Security, Vol.10, No.11, pp.9-17, 2018.

[27] P. R. da Cunha, P. Soja, and M. Themistocleous, “Blockchain for development: a guiding framework,” *Information Technology for Development*, vol. 27, no. 3. Routledge, pp. 417–438, 2021. doi: 10.1080/02681102.2021.1935453.

[28] P. Gupta, M. Hudnurkar, and S. Ambekar, “Effectiveness of blockchain to solve the interoperability challenges in healthcare,” *CARDIOMETRY*, no. 20, pp. 80–88, Nov. 2021, doi: 10.18137/cardiometry.2021.20.7987.

[29] S. Biswas, K. Sharif, F. Li, Z. Latif, S. S. Kanhere, and S. P. Mohanty, “Interoperability and Synchronization Management of Blockchain-Based Decentralized e-Health Systems,” *IEEE Trans Eng Manag*, vol. 67, no. 4, pp. 1363–1376, Nov. 2020, doi: 10.1109/TEM.2020.2989779.

[30] W. Viriyasitavat, L. Da Xu, Z. Bi, and A. Sapsomboon, “New blockchain-based architecture for service interoperations in internet of things,” *IEEE Trans Comput Soc Syst*, vol. 6, no. 4, pp. 739–748, Aug. 2019, doi: 10.1109/TCSS.2019.2924442.

[31] Omi Akter, Arnisha Akther, Md Ashraf Uddin, Md Manowarul Islam, " Cloud Forensics: Challenges and Blockchain Based Solutions", International Journal of Wireless and Microwave Technologies, Vol.10, No.5, pp. 1-12, 2020.

[32] G. M. George and L. S. Jayashree, “Ethereum Blockchain-Based Authentication Approach for Data Sharing in Cloud Storage Model,” *Cybern Syst*, 2022, doi: 10.1080/01969722.2022.2112544.

[33] G. Vasukidevi and T.Sethukarasi, “Blockchain Based Key Exchange Mechanism for Cloud Storage,” *Cybern Syst*, pp. 1–17, Jan. 2023, doi: 10.1080/01969722.2022.2157597.

[34] Rafael Belchior, Andre Vasconelos, Sergio Guerreiro, and Miguel Correia, “A Survey on Blockchain Interoperability: Past, Present, and Future Trends,” *ACM Computing Surveys (CSUR)*, vol. 54(8), pp. 1–41, 2021.

[35] S. Thota and G. K. Shyam, “Trends in building fungible blockchains for data and value exchange,” *International Journal of Blockchains and Cryptocurrencies*, vol. 2, no. 1, pp. 83–101, Jan. 2021, doi: 10.1504/IJBC.2021.117811.

[36] G. Wang, “SoK: Exploring Blockchains Interoperability,” *Cryptology ePrint Archive*, 2021, Accessed: Feb. 15, 2023. [Online]. Available: https://eprint.iacr.org/2021/537.pdf

[37] K. S. Alshudukhi, M. A. Khemakhem, F. E. Eassa, and K. M. Jambi, “An Interoperable Blockchain Security Frameworks Based on Microservices and Smart Contract in IoT Environment,” *Electronics (Switzerland)*, vol. 12, no. 3, Feb. 2023, doi: 10.3390/electronics12030776.

[38] E. R. D. Villarreal, J. Garcia-Alonso, E. Moguel, and J. A. H. Alegria, “Blockchain for Healthcare Management Systems: A Survey on Interoperability and Security,” *IEEE Access*, vol. 11, pp. 5629–5652, Jan. 2023, doi: 10.1109/access.2023.3236505.

[39] R. Belen-Saglam, E. Altuncu, Y. Lu, and S. Li, “A systematic literature review of the tension between the GDPR and public blockchain systems,” *Blockchain: Research and Applications*, p. 100129, Jan. 2023, doi: 10.1016/j.bcra.2023.100129.

[40] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, “A survey on privacy protection in blockchain system,” *Journal of Network and Computer Applications*, vol. 126. Academic Press, pp. 45–58, Jan. 15, 2019. doi: 10.1016/j.jnca.2018.10.020.

[41] Z. Wenhua, F. Qamar, T.-A. N. Abdali, R. Hassan, S. T. A. Jafri, and Q. N. Nguyen, “Blockchain Technology: Security Issues, Healthcare Applications, Challenges and Future Trends,” *Electronics (Basel)*, vol. 12, no. 3, p. 546, Jan. 2023, doi: 10.3390/electronics12030546.

[42] V. Malamas, P. Kotzanikolaou, T. K. Dasaklis, and M. Burmester, “A Hierarchical Multi Blockchain for Fine Grained Access to Medical Data,” *IEEE Access*, vol. 8, pp. 134393–134412, Jan. 2020, doi: 10.1109/ACCESS.2020.3011201.

[43] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, “A Survey on the Security of Blockchain Systems,” *Future Generation Computer Systems*, vol. 107, pp. 841–853, Feb. 2020, [Online]. Available: http://arxiv.org/abs/1802.06993

[44] Moonbeam Docs, “How to List your Project on State of the DApps.” https://docs.moonbeam.network/learn/dapps-list/state-of-the-dapps/ (accessed Mar. 18, 2023).

[45] Nimit Jain, Tarushi Agrawal, Pranav Goyal, and Vikas Hassija, “A Blockchain-Based distributed network for Secure Credit Scoring,” in *5th IEEE International Conference on Signal Processing, Computing and Control*, 5th IEEE International Conference on Signal Processing,Computing and Control, Oct. 2019.

[46] Margaret Reiter and Amy Loftsgordon, “The Nationwide Credit Reporting Agencies: Experian, Equifax, and TransUnion,” *Nolo*. https://www.nolo.com/legal-encyclopedia/the-nationwide-credit-reporting-agencies-experian-equifax-transunion.html (accessed Feb. 14, 2023).

[47] Dilip N, “The Risks of Blockchain on Credit Bureaus,” Supply Wisdom. https://www.supplywisdom.com/resources/the-risks-of-blockchain-on-credit-bureaus/ (accessed Feb. 14, 2023).

[48] Sruti Bhagavatula, Lujo Bauer, and Apu Kapadia, “What breach? Measuring online awareness of security incidents by studying real-world browsing behavior,” European Symposium on Usable Security, pp. 180–199, Oct. 2021, Accessed: Feb. 14, 2023. [Online]. Available: https://dl.acm.org/doi/fullHtml/10.1145/3481357.3481517

[49] “Experian.” https://www.experian.com/ (accessed Feb. 14, 2023).

[50] “Transunion credit bureau.” https://www.transunion.com/ (accessed Feb. 14, 2023).

[51] “5 Benefits of Colendi,” *Colendi*, 2018. https://medium.com/colendi/5-benefits-of-colendi-6a9a58fa3dd5 (accessed Feb. 14, 2023).

[52] Eray Eren, “Colendi Mobile ĐApp is live!,” *Colendi*, 2019. https://medium.com/colendi/colendi-mobile-%C3%B0app-is-live-e46591e398a1 (accessed Feb. 14, 2023).

[53] Pratik Bhakta & Ashwin Manikandan, “RBI restricts access to credit data of consumers,” *The Economic Times*, 2019. https://economictimes.indiatimes.com/small-biz/startups/newsbuzz/apex-bank-restricts-access-to-credit-data-of-consumers/articleshow/71194383.cms (accessed Feb. 15, 2023).

[54] “Government Gazette Republic of South Africa -No. 4 of 2013: Protection of Personal Information Act, 2013.,” Cape Town, 2013. Accessed: Feb. 14, 2023. [Online]. Available: https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013popi.pdf

[55] “The next generation credit bureau.” https://guppy.ai/about (accessed Feb. 15, 2023).

[56] Nick Galov, “40 Worrisome Hacking Statistics that Concern Us All in 2022,” *webtribunal*, Apr. 06, 2022. https://webtribunal.net/blog/hacking-statistics/#gref (accessed Feb. 15, 2023).

[57] Denys, “How the Consortium Blockchain Works,” *intellectsoft - Blockchain lab*, Sep. 25, 2019. https://blockchain.intellectsoft.net/blog/how-the-consortium-blockchain-works/ (accessed Feb. 15, 2023).

[58] W. Warren and A. Bandeali, “0x: An open protocol for decentralized exchange on the Ethereum blockchain,” 2017. Accessed: Feb. 14, 2023. [Online]. Available: https://github. com/0xProject/whitepaper

[59] “Regulatory compliance,” *Wikipedia*. https://en.wikipedia.org/wiki/Regulatory_compliance (accessed Feb. 14, 2023).

[60] T. C. W. Lin and T. C. Lin, “Compliance, Technology, and Modern Finance, 11 Brook,” 2016.

[61] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, “FHIRChain: Applying Blockchain to Securely and Scalably Share Clinical Data,” *Comput Struct Biotechnol J*, vol. 16, pp. 267–278, Jan. 2018, doi: 10.1016/j.csbj.2018.07.004.

[62] A. Leff and J. T. Rayfield, “Web-Application Development Using the Model/View/Controller Design Pattern,” in *Fifth IEEE International Enterprise Distributed Object Computing Conference*, 2001, pp. 118–127.

Authors’ Profiles

Surekha Thota obtained her M.Tech degree in Computer Networks and Information Security from G.Narayanamma Institute of Technology, Hyderabad, India and B.Tech from Sree Vidyanikethan Engineering College, Tirupati, India. She is currently pursuing her research in computer science engineering at REVA University, Bengaluru, India. Her major interests include Blockchain technologies, computer networks, cryptography and cyber security.

Shantala Devi Patil completed her B. E in Computer Science and Engineering from SDM college of Engineering and Technology(VTU), Dharwad and M.Tech in Computer Network and Engineering from Visvesvaraya Technological University Belagavi. She has completed her Ph.D in the area of security for Wireless Sensor Networks (WSNs) and Executive PG program in Data Science from IIIT, Bangalore. Presently, working as Associate Professor and Program Head (Artificial intelligence and Data Science) in School of Computing and Information technology, REVA University, Bangalore. Her areas of interest include Networks, IoT, Data Science and Behavioral Science.

Gopal Krishna Shyam received B.E., M.Tech and PhD Degree in Computer Science & Engg. from Visveswaraya Technological University, Belagavi. He is currently working as a Professor and HoD in School of Computer Engineering, Presidency University, Bengaluru, India. His research areas include Cloud/Grid computing, E-commerce, Protocol engineering, and Artificial intelligence applications.

Bhanu Prasad received Master of Technology and Ph.D. degrees, both in computer science, from Andhra University and Indian Institute of Technology Madras, respectively. He is currently serving as a Professor in the Department of Computer and Information Sciences at Florida A&M University in Tallahassee, Florida, USA. His research interests include Artificial Intelligence and Software Engineering.

How to cite this paper: Surekha Thota, Shantala Devi Patil, Gopal Krishna Shyam, Bhanu Prasad, "GDAR: A Secure Authentication for Dapp Interoperability in Blockchain", International Journal of Computer Network and Information Security(IJCNIS), Vol.16, No.6, pp.69-82, 2024. DOI:10.5815/ijcnis.2024.06.06