IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 2 May 2024, accepted 4 July 2024, date of publication 15 July 2024, date of current version 30 July 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3427805

RESEARCH ARTICLE

Ethereum Blockchain Framework Enabling Banks to Know Their Customers

C. VINOTH KUMAR[1], POONGUNDRAN SELVAPRABHU[1], NIVETHA BASKA[1], U. VIVEK MENON[1], VINOTH BABU KUMARAVELU[1], (Senior Member, IEEE), SUNIL CHINNADURAI[2], (Senior Member, IEEE), AND FARMAN ALI[3]

[1]Department of Communication Engineering, School of Electronics Engineering (SENSE), Vellore Institute of Technology, Vellore, Tamil Nadu 632014, India
[2]Department of Electronics and Communication Engineering, School of Engineering and Applied Sciences, SRM University-AP, Amaravati, Andhra Pradesh 522502, India
[3]Department of Applied AI, Sungkyunkwan University, Seoul 03063, South Korea

Corresponding author: Poongundran Selvaprabhu (poongundrano7@gmail.com; poongundran.selvaprabhu@vit.ac.in)

This work was supported by the School of Electronics Engineering (SENSE), Vellore Institute of Technology, Vellore, Tamil Nadu, India.

ABSTRACT The Know Your Customer (KYC) process is a fundamental prerequisite for any financial institution's compliance with the regulatory framework. Blockchain technology has emerged as a revolutionary solution to enhance the effectiveness of the KYC procedure. It ensures that the KYC process is transparent, secure, and immutable, thereby offering a robust solution to combat fraudulent activities. The potential of blockchain technology in revolutionizing the KYC process has been acknowledged globally. Blockchain technology provides a decentralized platform for storing customer data, enabling financial institutions to access the information seamlessly. Using ethereum blockchain technology in KYC procedures can enhance the efficiency of financial institutions, significantly reducing the time and cost associated with the process. This work aims to provide a viable and sustainable solution to the challenges that banks experience in implementing KYC procedures and onboarding new customers. The proposed solution involves the central bank maintaining a comprehensive register of all registered banks while closely monitoring their adherence to the existing regulations governing KYC and customer acquisition.

INDEX TERMS Blockchain, decentralized, ethereum, immutable, KYC, secure.

I. INTRODUCTION

The central banks and other governmental financial institutions face significant challenges in effectively tracking money laundering activities, particularly those that are linked to terrorism and other criminal activities. Money laundering (ML) has become a global issue, and it is estimated that approximately $2 trillion is laundered each year [1]. The failure to tackle this issue poses a serious threat to national security. It can harm the economy and undermine the financial system's integrity. The methods used by money launderers have become increasingly sophisticated, making it difficult for regulators and financial institutions to detect them. Criminals often use complex financial structures and multiple transactions to conceal their activities. Moreover, money laundering is often linked to other criminal activities, such as drug trafficking, human trafficking, and corruption [2].

Given the complexities involved in detecting and preventing money laundering, it is imperative that regulators and financial institutions collaborate closely to implement effective measures to combat this issue. Such measures may include increased transparency and reporting requirements, enhanced due diligence procedures, and improved information sharing. Financial institutions must also ensure that their staff are adequately trained to identify and report suspicious activity. Failure to tackle the issue of money laundering could result in significant reputational and financial damage to businesses and countries alike. Hence, it is vital that all stakeholders work together to combat this global menace and safeguard the integrity of the global financial system [3], [4]. The International Monetary Fund (IMF) recommends allocating resources in a targeted manner to prevent money laundering and terrorist financing effectively. To achieve this,

The associate editor coordinating the review of this manuscript and approving it for publication was Mansoor Ahmed.

FIGURE 1. IMF support for risk assessment in detecting money laundering and terrorist financing.

focusing on areas where resources will be most impactful is essential. Figure 1 provides a visual representation of such areas. By prioritizing these areas, organizations can ensure that their resources are used effectively and efficiently to combat financial crimes [5]. This necessitates a thorough analysis and understanding of the risks associated with ML and terrorist financing (TF) in the country. This analysis should consider a wide range of factors, such as the types of financial services and products available, the vulnerabilities of different sectors and industries to ML/TF, and the prevalence of different ML/TF methods and techniques. Armed with this information, authorities can devise and implement targeted measures to address these risks, such as enhanced due diligence requirements, increased monitoring and reporting obligations, and stricter enforcement measures. A risk-based approach focusing on the most significant threats is crucial for effective ML/TF prevention. To safeguard the financial system's integrity and prevent its exploitation for illicit purposes, countries must also stay ahead of the evolving tactics and techniques of those who engage in ML/TF. This requires ongoing analysis and adjustment of strategies to address new threats.

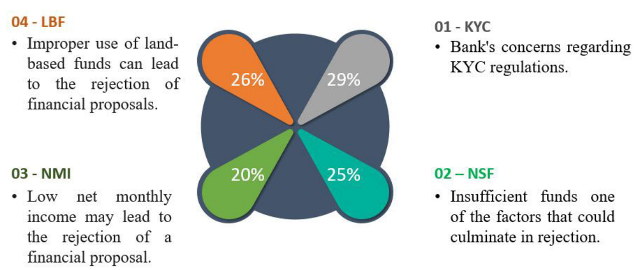

FIGURE 2. The factors behind banks refusal of commercial financing proposals.

As shown in figure 2 when submitting a commercial financing proposal to a bank, it's essential to understand the factors that may lead to rejection. One of the primary reasons for rejection is the bank's concerns regarding KYC regulations. Therefore, providing all necessary documents and fulfilling the KYC requirements can increase the chances of approval. Another factor that may lead to rejection is no sufficient funds (NSF). In such cases, presenting a well-thought-out financial plan to demonstrate how the funds will be utilized can help increase the chances of approval. Additionally, inappropriate land-based funds (LBF) and low net monthly income (NMI) can also lead to rejection. Another common reason for rejection is inadequate credit history. Banks may also decline financing proposals if the business has weak cash flow or profitability, suggesting it may struggle to meet its financial obligations. A risky business model or a subpar business plan can also contribute to a proposal being rejected [6], [7].

In addition to these factors, banks may also consider external elements such as economic conditions or industry trends before approving or rejecting financing proposals. For instance, if the economy is experiencing a downturn, banks may be more cautious about extending credit to businesses. Similarly, they may be less likely to approve financing for businesses operating in sectors that are experiencing a decline. However, businesses can take several measures to improve their chances of securing financing from banks. By building a strong credit history, businesses can demonstrate their financial stability and credibility to banks. Optimizing cash flow and developing a sound business plan can also help businesses present themselves as viable and attractive candidates for financing [8], [9]. Furthermore, businesses must stay informed about economic conditions and industry trends, allowing them to tailor their financing proposals to align with market realities. By addressing these factors proactively, businesses can overcome obstacles, increase their chances of securing bank financing, and ultimately achieve their financial objectives.

As shown in figure 3, traditional KYC is a process that necessitates a face-to-face interaction to verify a customer's identity. As part of this process, customers provide physical identification documents, such as ID cards or passports, to a financial institution for verification purposes. The primary objective of "Traditional KYC" is to ensure that the customer is who they claim to be and to prevent identity theft or fraud. The traditional KYC process, used to verify the identity of clients, has encountered significant challenges regarding the establishment of mechanisms that prioritize privacy when sharing KYC data. Additionally, there is a notable absence of universally accepted security standards within this process. During the process, the customer's physical documents are thoroughly examined and evaluated to ensure that the information provided is accurate [10]. Financial institutions use their internal databases to check the information provided by customers to prevent fraudulent activities. Compliance with financial regulations and laws is essential for every financial institution, and the traditional KYC process is an integral part of ensuring that such compliance is achieved. By following this process, financial institutions build trust with their customers and provide a secure and reliable service. Traditional KYC verifies your identity with physical documents like IDs or passports at a bank [11], [12].

However, the traditional KYC process in banking is not without limitations. Some of the drawbacks include the high cost of implementation, the time-consuming nature of the process, and the potential for errors and inaccuracies due to manual data entry. Additionally, the requirement for customers to physically visit a bank branch or submit paper-based documents for verification can be inconvenient and burdensome [13]. These limitations can result in a less-than-ideal customer experience, ultimately affecting customer retention and satisfaction. Therefore, it is important to address these limitations and adopt more efficient and effective KYC processes that leverage technology such as blockchain, artificial intelligence, and biometric authentication [14]. These technologies can help streamline the process, reduce costs, and improve accuracy while providing a more convenient and secure experience for customers [15], [16].

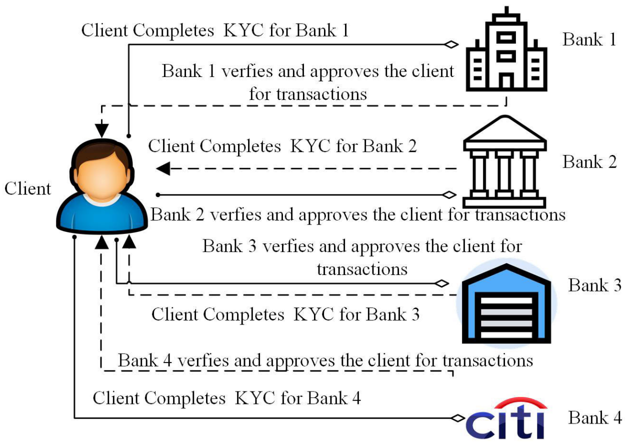

FIGURE 3. Traditional KYC the process that necessitates a face-to-face interaction to verify a customer's identity.

A. STRUCTURE OF THE WORK

This paper will present a comprehensive and detailed analysis of the chosen topic. The introduction will give readers a complete comprehension of the subject area. Additionally, the following sections will aid in making understanding easier. Section I explores the various factors affecting the KYC process and proposes using blockchain technology to enhance the traditional process. Section II provides an extensive review of the existing literature on the KYC process, aiming to offer a thorough understanding of the research conducted in this field. By delving into Section III, we can gain a deeper understanding of how the proposed system will be brought to life, inspiring us to take the necessary steps toward making it a reality. Section IV of the report discusses the testing and validation process of the proposed system on the ethereum blockchain. Section V discusses the conclusions drawn from the research and potential future work.

II. RELATED WORKS

In work paper [17], Kapsoulis et al. have developed an innovative KYC document validation scheme based on IPFS and blockchain technology. The system requires consumers to provide their identity details to the lender, and their information is then encrypted and secured using gpg4win encryption software. However, it is worth noting that the article fails to address significant concerns around the confidentiality and reliability of transactions. In work paper [18], Sai et al. suggested a blockchain KYC system modeled after the microfinance system. The proposed system was tested in private blockchain scenarios using Polygon, an enormously distributed platform. In an article [19], Norvill et al. proposed a framework which enables automation and permission document sharing over the blockchain to streamline the KYC process.

In a research paper [20], Ullah et al. suggested a Hyperledger Fabric network that optimizes the KYC process. In this model, the customer has complete ownership rights of the smart contracts that contain their KYC data in the distributed ledger database. Nevertheless, the work does not focus on the confidentiality and key management factors of the KYC process. In this article [21], Karadag et al. suggest the blockchain-based KYC model, which illustrates the transparent sharing of loan allocation data for bank customers who have received loans. The paper discusses the challenges posed by the rapid growth of global data, highlighting the need for secure storage and effective sharing among stakeholders. While regulatory obstacles exist, the potential for improved efficiency, collaboration, and risk management within a secure and transparent framework is evident. In this article [22], Thommandru et al. discuss compliance and Anti-Money Laundering (AML) policies in the banking sector, focusing on the use of new emerging technologies such as blockchain. The paper addresses issues related to the manipulation of KYC and the financial burden on banks while also addressing AML policies. Finally, the paper provides ideas and suggestions on how emerging technologies such as blockchain can be utilized to address the problems of money laundering. This includes the potential for blockchain technology to recalibrate banking systems' compliance policies. In this work [23], Yadav et al. discuss a KYC system powered by blockchain technology that has been developed to enhance the existing KYC process. However, the article fails to adequately address the necessary checks and balances required to ensure the integrity and security of the system. The inclusion of such measures is crucial in mitigating the risks associated with the use of this technology and promoting its wider adoption.

- The novel technique presented by the suggested decentralized KYC model can significantly minimize the time people must engage with one another during the KYC verification process.
- This paradigm restricts the submission of individual documents to various organizations to address the problem of data leaks.
- The core bank maintains a comprehensive registry of all registered banks, while closely monitoring their adherence to existing regulations governing KYC and customer acquisition. This is a critical function that ensures the stability and safety of the financial system.

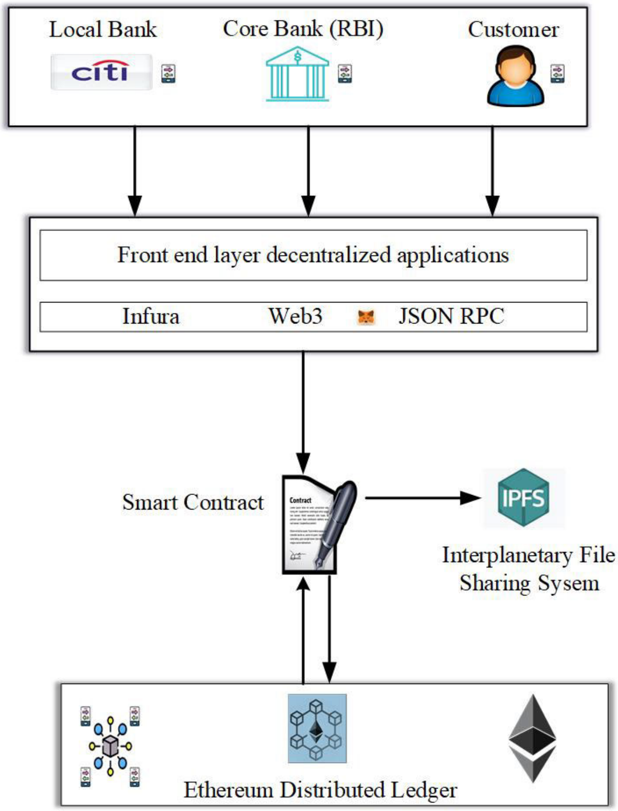

FIGURE 4. Implementation of a blockchain-based KYC process.

Blockchain technology makes it impossible for any party to default on a transaction and ensures that every transaction is highly resistant to change. The decentralization of the KYC procedure is a significant advancement over current models and can potentially increase the security and efficiency of the verification process. Through the utilization of Blockchain technology and decentralization, we can establish a KYC verification method that is dependable, efficient, and safe.

III. IMPLEMENTATION

Many industries, particularly the financial and banking communities, are interested in blockchain technology due to its many advantages. One area of growing interest is using e-KYC platforms that leverage blockchain and cloud systems. As shown in figure 4, This technology offers a decentralized structure that promotes transparency, agility, trustworthiness, and affordability for transactional analysis and management in multiple user and provider environments. The blockchain system is a distributed database that allows multiple users to access and update data, ensuring that all parties have access to the same information and that it is up-to-date [24]. This transparency and data encryption makes it highly secure and trustworthy. Moreover, the decentralized structure of blockchain enables faster transaction processing and management, reducing the need for intermediaries and the costs associated with their services.

Blockchain technology has a contract feature that makes it possible to execute distributed logic. This feature improves the usability and flexibility of systems that operate on the blockchain network. It enables the routine and automated execution of distributed operations on a decentralized network, which makes the system more secure and reliable. [25], [26]. Self-executing programs are a powerful solution for optimizing processes and increasing efficiency. With their ability to automatically perform specific tasks, intermediaries become redundant, and processing time is significantly reduced [27]. By implementing these programs, we can confidently expect a more streamlined workflow and a boost in productivity. This feature, combined with the security and transparency of blockchain, makes it an ideal technology for transaction processing and management.

Figure 5 describes a sequential flow diagram that showcases the proposed KYC process using blockchain technology. The diagram provides a clear and concise overview of the various steps involved in the process, highlighting how blockchain technology can be leveraged to make KYC more secure and efficient. The proposed KYC process is an innovative approach that offers significant benefits, such as reduced costs and time associated with traditional KYC processes, improved accuracy, transparency, and privacy of customer data, and enhanced compliance processes. By adopting this advanced approach to KYC, businesses can streamline their operations, improve customer satisfaction, and gain a competitive edge in their respective industries. The diagram is a valuable resource that can help businesses better understand the KYC process utilizing blockchain technology and its potential to revolutionize how we manage customer data.

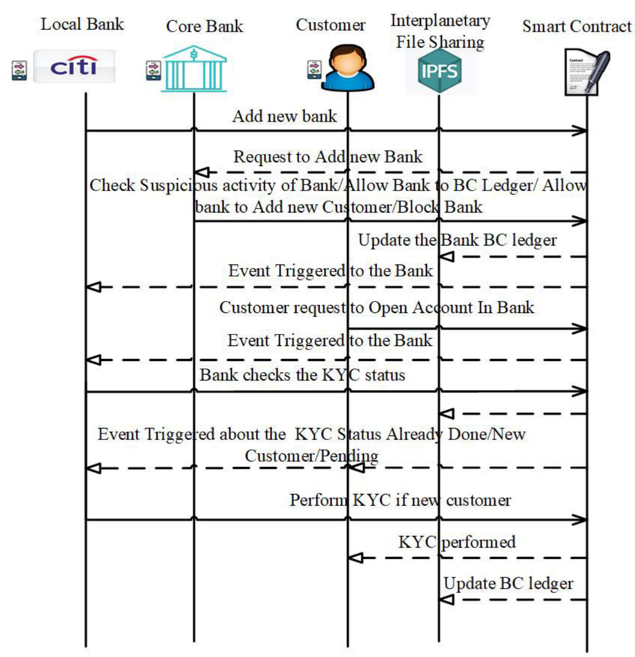

FIGURE 5. Sequential flow diagram illustrating the proposed KYC process using blockchain technology.

Algorithm 1 Mandatory Requirements in the Process

Input: Bank name, Bank Address
require(!areStringSame(banks[add].name,bankName), "A Bank already exists with same name") ⋆ ⟶ **Step-1**
banks[add] = Bank(bankName,0,add,true,true)
Output: An event declaring whether the bank is already existing or not
/* Allow Bank to do KYC */
Input: Bank Address
require(banks[add].Address != address(0), "Bank not found") ⋆ ⟶ **Step-2**
banks[add].kycPrivilege = true
return 1
Output: Previliged Bank to do KYC /* Allow bank to add new customer */
Input: Bank Address
require(banks[add].Address != address(0), "Bank not found") ⋆ ⟶ **Step-3**
require(!banks[add].isAllowedToAddCustomer, "Requested Bank is already allowed to add new customers")
banks[add].isAllowedToAddCustomer = true
return 1
Output: Bank is allowed to add new customer /* Block Bank to do KYC */
Input: Bank Address
require(banks[add].Address != address(0), "Bank not found") ⋆ ⟶ **Step-4**
banks[add].kycPrivilege = false
return 1
Output: KYC Privilege is not given to this bank
/* Block Bank to add new customer */
Input: Bank Address
require(banks[add].Address != address(0), "Bank not found") ⋆ ⟶ **Step-5**
require(banks[add].isAllowedToAddCustomer, "Requested Bank is already blocked to add new customers")
banks[add].isAllowedToAddCustomer = false
return 1
Output: Bank is blocked to add new customer
/* Add new customer to Bank */
Input: Customer Name, Customer Hash ⋆ ⟶ **Step-6**
require(banks[msg.sender].isAllowedToAddCustomer, "Requested Bank is blocked to add new customers")
require(customersInfo[custName].validatedBank == address(0), "Requested Customer already exists")
customersInfo[custName] = Customer(custName, custData,msg.sender,false)
Output: Customer Name, Customer Hash,Customer Already Exists, Bank is not allowed to add customer

Algorithm 1 represents the set of essential requirements that administrators must provide when setting up a new banking system. These requirements are designed to ensure the integrity and security of transactions carried out within the system. The bank name is the official name of the financial institution being represented and must be provided. This information is essential for customers to identify the bank they are dealing with. The unique ethereum address of the bank is also mandatory. This address serves as a decentralized and secure way of tracking transactions within the system. The ethereum blockchain technology ensures that all transactions are recorded and cannot be altered or deleted, making it a reliable way to track financial activities. Finally, the customer unique identification number is a unique identifier for each customer. This number is used to protect the customer's identity and ensure that their transactions are secure. By providing all of these mandatory requirements, administrators can create a safe, reliable, and secure banking system for their customers.

When adding a new bank to the blockchain network, the administrator first checks the unique ethereum address of the bank to verify if it is already listed in the ledger. This process is important to maintain the integrity and security of the network. If the ethereum address of the new bank matches an existing address, an event is triggered to notify the administrator that "A bank already exists with the same name." Conversely, if the addresses do not match, the new bank is added to the network. This careful consideration ensures that no duplicate banks are added to the blockchain network, thereby contributing to its overall efficiency and effectiveness. The subsequent step in the administrative process necessitates the authorization of banks to carry out KYC procedures and add new customers to their respective institutions. If an invalid ethereum address is provided by the bank, an event will be triggered with the message "Bank Not Found". Conversely, if the address is valid, KYC privileges will be granted with a true condition, and "Requested bank is allowed to add customer" will be triggered. It is imperative that the bank provides a valid ethereum address to enable the smooth execution of the KYC process.

In the next step, when the administrator encounters any miscellaneous issues with the banks in the enrolled list or newly approached banks that need to be added to the ledger, they can take the necessary action to prevent such issues from occurring. The administrator can block the bank's ethereum address, preventing the bank from performing KYC and adding new customers. This will ensure that the bank does not create any more problems in the system. To implement this, the administrator can trigger an event that displays the message "Requested Bank is already blocked to add new customers" and sets the KYC privilege to false. This will prevent the bank from adding new customers until the issue is resolved. Once the issue is resolved, the administrator can unblock the bank's ethereum address and restore its KYC privilege.

Algorithm 2 is a highly sophisticated system designed to provide comprehensive information on a customer's KYC status, including their name and other relevant details. The system is accessed by inputting the customer's name, after

Algorithm 2 Status and Viewing Customer Information

Input: Name of the Customer
require(banks[msg.sender].kycPrivilege, "Requested Bank does not have KYC Privilege" $\star \longrightarrow$ **Step-1**
customersInfo[custName].kycStatus= true
Output: Boolean, Bank do not have Previlege /* Call Customer Data */
Input: Name of the Customer
require(customersInfo[custName].validatedBank != address(0), "Requested Customer not found") $\star \longrightarrow$ **Step-2**
return (customersInfo[custName].data, customersInfo[custName].kycStatus)
Output: Customer Not found, Status of the Customer /* Know your Customer Status */
Input: Name of the Customer
require(customersInfo[custName].validatedBank != address(0), "Requested Customer not found") $\star \longrightarrow$ **Step-3**
return (customersInfo[custName].kycStatus)
Output: Boolean, Customer requested not found /* To check whether the bank already exists */
If(bytes(a).length != bytes(b).length) then
    return false $\star \longrightarrow$ **Step-4**
else
    return
  keccak256(bytes(a)) == keccak256(bytes(b))
end

which algorithm 2 computes the KYC status and generates a boolean value that confirms the customer's compliance status. A true value confirms the customer meets the KYC requirements, while a false value indicates that more information is required. Algorithm 2 is designed to be user-friendly, with tailored outputs for different scenarios when the KYC status is false. For example, when the requested customer's details are unavailable in the system, the output "Requested customer not found" is returned. If the bank does not have the privilege to access the information, the output "Bank does not have the privilege" is produced. Finally, if further information is required on the customer's KYC compliance status, the output "KYC status" is returned.

IV. TESTING AND VALIDATION

Once the contract is deployed, the administrator is granted the power to add new banks to the blockchain network. This is facilitated by executing the "addNewBank" function as shown in figure 6, which requires two inputs - the bank's name and a unique Ethereum address of 0 × 5B38Da6a701c568545dCfcB03FcB875f56beddC4. Adding new banks to the network is a crucial function that ensures secure and efficient fund transfers between different banks on the blockchain. The successful execution of the "addNewBank" function adds a new bank to the blockchain network, facilitating seamless communication and fund

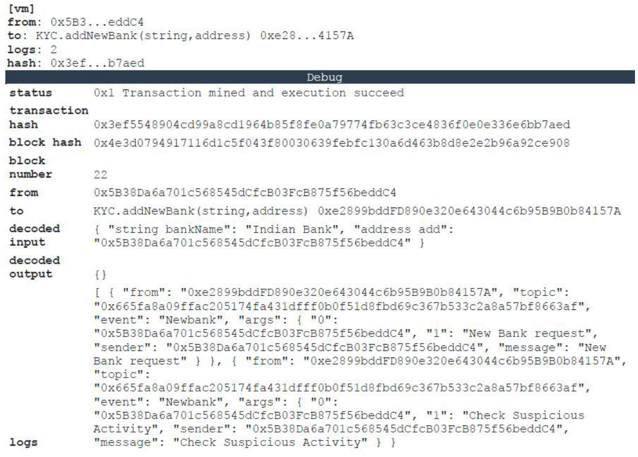

FIGURE 6. Successful execution of adding a new bank function.

transfer between banks. The integration of new banks into the network is essential for maintaining an updated and efficient network, ensuring a smooth experience for all users. By adding new banks to the network, the blockchain network stays up-to-date, and users can enjoy the benefits of secure and efficient fund transfer. The "addNewBank" function is a constructive feature that promotes the growth and development of the blockchain network, making it a reliable and efficient platform for all users. Once the bank has been successfully added, the admin will be granted the authority to enable the KYC function for them. This function is crucial in verifying customers' identities and ensuring compliance with regulatory guidelines. To enable the KYC function, the admin must use the unique ethereum address 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4. This address is specific to this KYC process and associated with the bank's identity. The admin will initiate the transaction to enable the KYC function, as shown in figure 7, which will then be confirmed and verified by the ethereum network. Once the transaction is successfully executed, the bank will be authorized to perform the KYC function. The bank will be able to ensure that the customer's identity is legitimate and complies with the regulatory guidelines.

FIGURE 7. Successful execution of Allow bank to perform KYC function.

In the event of an instance where a bank is discovered to be violating the guidelines established by the reserve bank of

India, the administrator will be bestowed with the authority to disable its KYC function. To disable the KYC function, the administrator must employ a unique ethereum address, which has been specifically designated for the KYC process and is linked to the bank's identity. The ethereum network address 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4 identifies the KYC process associated with the bank. The administrator shall initiate a transaction to disable the KYC function, which is successfully executed as shown in figure 8.

```
[vm]
from: 0x5B3...eddC4
to: KYC.blockBankFromKYC(address) 0xd91...39138
value: 0 wei
data: 0x9de...eddc4
logs: 0
hash: 0xc9c...fe68c
                                Debug
status            0x1 Transaction mined and execution succeed
transaction hash  0xc9ca3b6242e89437a3bcd53b5b9bf4bbcb902ba6cd4543f7533d02558defe68c
block hash        0x73651add4ed80b0833179927a33107ec57b6f3386b0f05f405757bdaf11597f8
block number      17
from              0x5B38Da6a701c568545dCfcB03FcB875f56beddC4
to                KYC.blockBankFromKYC(address) 0xd9145CCE52D386f254917e481eB44e9943F39138
gas               33851 gas
transaction cost  29435 gas
execution cost    8003 gas
input             0x9de...eddc4
decoded input     { "address add": "0x5B38Da6a701c568545dCfcB03FcB875f56beddC4" }
decoded output    { "0": "int256: 1" }
```

FIGURE 8. Successful execution of Blocking banks to do KYC.

```
revert
    The transaction has been reverted to the initial state.
Reason provided by the contract: "Requested Bank does'nt have KYC Privilege".
Debug the transaction to get more information.
[vm]
from: 0x5B3...eddC4
to: KYC.addNewCustomerRequestForKYC(string) 0xd91...39138
value: 0 wei
data: 0x211...00000
logs: 0
hash: 0x78a...a72b3
                                Debug
status            0x0 Transaction mined but execution failed
```

FIGURE 9. Successful execution of Kyc Privilege function.

Upon successful execution of the transaction, the bank's KYC function will be disabled. As a result, the bank will be unable to perform any KYC checks until the administrator re-enables the function as shown in figure 9 highlighting "Requested bank doesn't have KYC privilege" and figure 10 represents successful execution of "Requested bank is blocked to add new customer to bank." It is crucial to note that disabling the KYC function is a significant measure and should solely be employed in instances where the bank is discovered to be in violation of regulations. This is due to the fact that KYC is a fundamental aspect of ensuring financial transparency and preventing ML.

```
revert
    The transaction has been reverted to the initial state.
Reason provided by the contract: "Requested Bank is blocked to add new customers".
Debug the transaction to get more information.
[vm]
from: 0x5B3...eddC4
to: KYC.addNewCustomerToBank(string,string) 0xd91...39138
value: 0 wei
data: 0x284...00000
logs: 0
hash: 0x832...0f76e
                                Debug
status            0x0 Transaction mined but execution failed
```

FIGURE 10. Successful execution of the requested bank is blocked to add a customer.

```
[vm]
from: 0x5B3...eddC4
to: KYC.addNewCustomerToBank(string,string) 0xd91...39138
value: 0 wei
data: 0x284...00000
logs: 0
hash: 0xea2...fe253
                                Debug
status            0x1 Transaction mined and execution succeed
transaction hash  0xea2519a40035503be2013ee7dd9839748219d99679348f69b4d57217ffbfe253
block hash        0xada38084f85fe335aecb2ace6ca08f3a5a160f1bdb1cffe3b756813dccd446e7
block number      16
from              0x5B38Da6a701c568545dCfcB03FcB875f56beddC4
to                KYC.addNewCustomerToBank(string,string) 0xd9145CCE52D386f254917e481eB44e9943F39138
gas               107711 gas
transaction cost  93661 gas
execution cost    71541 gas
input             0x284...00000
decoded input     { "string custName": "Swaru", "string custData": "9459438t93ut93u" }
```

FIGURE 11. Successful execution of adding a new customer function.

When a bank is authorized to add a new customer to its database, it follows a strict process to ensure that the customer's personal information is collected and verified accurately. This includes details such as the customer's full name and a unique identification number. Once this information is confirmed, the bank can then proceed to create a new account and add the customer to its records. Figure 11 provides a visual representation of the successful execution of the process of adding a new customer to the bank's records. This indicates that the KYC process has been completed successfully and the customer's information has been added to the bank's database if the KYC status is true, as shown in figure 12. The verification process is crucial as it ensures that the bank's database is accurate and up-to-date while also protecting the customer's personal information. However, if the bank rejects the KYC process, the status will be false.

```
call to KYC.getCustomerKycStatus
CALL[call]
from: 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4
to: KYC.getCustomerKycStatus(string)
data: 0x761...00000
                                Debug
from              0x5B38Da6a701c568545dCfcB03FcB875f56beddC4
to                KYC.getCustomerKycStatus(string) 0xd9145CCE52D386f254917e481eB44e9943F39138
execution cost    3610 gas (Cost only applies when called by a contract)
input             0x761...00000
decoded input     { "string custName": "Vino" }
decoded output    { "0": "bool: true" }
```

FIGURE 12. Successful execution of Know your customer status.

If, during the course of database operations, it is found that a customer is already present in the database, the "requested customer already exists" trigger will be executed. This trigger is intended to alert the system that the customer already exists and avoid duplication or conflicting data entries. The successful execution of this trigger is depicted in figure 13 and indicates that the system is functioning as intended and that customer data is being processed accurately. If the customer is not found in the database, the system will provide a message indicating, "Requested customer not found," as shown in figure 14. This can help the user double-check the customer's details and ensure the correct information was entered.

Once all the mandatory KYC processes have been completed, authorized personnel within the blockchain network can access customer information by calling up the customer data. This information is stored in a secure and tamper-proof manner on the blockchain, ensuring that it cannot be

```
transact to KYC.addNewCustomerToBank errored: Error occurred: revert.

revert
    The transaction has been reverted to the initial state.
Reason provided by the contract: "Requested Customer already exists".
Debug the transaction to get more information.
[vm]
from: 0x5B3...eddC4
to: KYC.addNewCustomerToBank(string,string) 0xd91...39138
value: 0 wei
data: 0x284...00000
logs: 0
hash: 0xe58...eda77
                                    Debug
status          0x0 Transaction mined but execution failed
```

FIGURE 13. Successful execution of customer already exists.

```
call to KYC.getCustomerKycStatus errored: Error occurred: revert.

revert
      The transaction has been reverted to the initial state.
Reason provided by the contract: "Requested Customer not found".
Debug the transaction to get more information.
```

FIGURE 14. Successful execution of customer not found.

```
call to KYC.viewCustomerData
CALL[call]
from: 0x5B38Da6a701c568545dCfcB03FcB875f56beddC4
to: KYC.viewCustomerData(string)
data: 0x4a6...00000
                                    Debug
from             0x5B38Da6a701c568545dCfcB03FcB875f56beddC4
to               KYC.viewCustomerData(string) 0xd9145CCE52D386f254917e481eB44e9943F39138
execution cost   6909 gas (Cost only applies when called by a contract)
input            0x4a6...00000
decoded input    { "string custName": "Vino" }
decoded output   { "0": "string: 9459438t93ut93u", "1": "bool: true" }
```

FIGURE 15. Successful execution of viewing the customer information.

modified or deleted without proper authorization. Figure 15 demonstrates the successful execution of viewing customer data, highlighting key details such as the customer's name and unique ID. This process provides a convenient and efficient way for parties within the blockchain network to access customer information without compromising security or privacy.

A. VULNERABILITY ANALYSIS

Malicious actors may be able to take advantage of programming defects or mistakes in smart contracts. These flaws may give rise to illegal access into the contract or the ability to change its terms, which could result in significant financial loss or other harm, particularly if the smart contracts are utilized for important or financial transactions. Therefore, to reduce the hazards linked with these vulnerabilities, it is imperative to make sure that smart contracts undergo thorough testing and auditing before being deployed in any real-world situation. As shown in figure 16, the oyente smart contract analyzer was used to perform a comprehensive analysis of the system's security. The analyzer has conducted a thorough assessment and has identified potential vulnerabilities in specific areas of the system. After conducting a thorough analysis, it has been determined that no actual vulnerabilities exist or the reported vulnerabilities are false.

```
tt144@tt144lab-HP-Pro-SFF-280-G9-Desktop:~$ sudo docker run -i -t luongnguyen/oyente
root@ec204145e2ed:/oyente# cd /oyente/oyente
root@ec204145e2ed:/oyente/oyente# python oyente.py -s kyc.sol
WARNING:root:You are using evm version 1.8.2. The supported version is 1.7.3
WARNING:root:You are using solc version 0.4.21, The latest supported version is 0.4.19
INFO:root:contract kyc.sol:kyc:
INFO:symExec:     ============ Results ===========
INFO:symExec:      EVM Code Coverage:                         99.2%
INFO:symExec:      Integer Underflow:                         False
INFO:symExec:      Integer Overflow:                          False
INFO:symExec:      Parity Multisig Bug 2:                     False
INFO:symExec:      Callstack Depth Attack Vulnerability:      False
INFO:symExec:      Transaction-Ordering Dependence (TOD):     False
INFO:symExec:      Timestamp Dependency:                      False
INFO:symExec:      Re-Entrancy Vulnerability:                 False
INFO:symExec:     ====== Analysis Completed ======
root@ec204145e2ed:/oyente/oyente#
```

FIGURE 16. Successful execution of vulnerability analysis of smart contract.

- Integer overflow and underflow: This vulnerability occurs when a mathematical operation results in a value that is too large or too small to be stored by the system.
- Parity multisig bug 2: This vulnerability was discovered in the parity multi-sig wallet and allowed an attacker to gain control of the wallet's funds.
- Call stack depth attack: This vulnerability occurs when a malicious actor exploits the system's call stack to cause it to overflow and crash.
- Transaction ordering dependency: This vulnerability occurs when the outcome of a transaction depends on the order in which it is processed by the system.
- Timestamp dependency: This vulnerability occurs when a transaction's outcome depends on the timestamp at which it was executed.
- Re-entrance: This vulnerability allows an attacker to repeatedly call a function before it has finished executing, potentially causing the system to crash.

V. CONCLUSION

In this paper, we have presented a revolutionary solution to the long-standing problem of KYC using blockchain technology. The proposed KYC process is designed to meet the requirements of modern businesses. Utilizing the strengths of blockchain, such as distributed ledger and immutability, we have created a solution far superior to existing ones. Therefore, this blockchain-based solution ensures that unauthorized entities cannot modify sensitive KYC data, which is an advantage over existing solutions. Moreover, it is cost-effective for the companies, significantly reducing infrastructure costs. Our solution also eliminates the need for users to repeat the KYC process once they have entered the system, saving valuable time and effort. The decentralized peer-to-peer network of the proposed system offers several advantages over centralized ones, making it more secure against vulnerability attacks. We have even simulated a scenario where a bank might not trust other banks in the network and solve it using digital signatures. The solution from the proposed work ensures that authorized entities always validate the KYC process and that the data remains unaltered. With our blockchain-based KYC solution, businesses can ensure that their KYC process is secure, efficient, and cost-effective.

In the foreseeable future, our objective is to deploy and conduct testing of our solution on the real ethereum network. Moreover, we aim to develop a comprehensive, fully operational decentralized application (DApp). This would entail a meticulous examination of the technical feasibility of the proposed solution on the ethereum network, an evaluation of the potential for adoption, and a thorough assessment of the security and privacy implications of the DApp. The ultimate goal is to establish a robust and reliable DApp that can deliver a seamless user experience while ensuring transparency, security, and efficiency.

REFERENCES

[1] H. Alanzi and M. Alkhatib, "Towards improving privacy and security of identity management systems using blockchain technology: A systematic review," *Appl. Sci.*, vol. 12, no. 23, p. 12415, Dec. 2022.

[2] Y. Chen, Y. Lu, L. Bulysheva, and M. Y. Kataev, "Applications of blockchain in Industry 4.0: A review," *Inf. Syst. Frontiers*, vol. 24, pp. 1–15, Feb. 2022.

[3] M. N. M. Bhutta, A. A. Khwaja, A. Nadeem, H. F. Ahmad, M. K. Khan, M. A. Hanif, H. Song, M. Alshamari, and Y. Cao, "A survey on blockchain technology: Evolution, architecture and security," *IEEE Access*, vol. 9, pp. 61048–61073, 2021.

[4] J. Dorminey, A. S. Fleming, M.-J. Kranacher, and R. A. Riley, "The evolution of fraud theory," *Issues Accounting Educ.*, vol. 27, no. 2, pp. 555–579, May 2012.

[5] (2024). *IMF Assessment*. Accessed: Mar. 3, 2024. [Online]. Available: https://www.imf.org/en/Publications/fssa

[6] F. C. Hui, V. C. Koneru, N. M. Ali, and S. Harun, "Implementing peer group analysis within a track and trace system to detect potential frauds," *Int. J. Supply Chain Manage.*, vol. 3, pp. 52–56, Jan. 2014.

[7] R. Patel, M. Migliavacca, and M. E. Oriani, "Blockchain in banking and finance: A bibliometric review," *Res. Int. Bus. Finance*, vol. 62, Dec. 2022, Art. no. 101718.

[8] Q. Gan, R. Y. K. Lau, and J. Hong, "A critical review of blockchain applications to banking and finance: A qualitative thematic analysis approach," *Technol. Anal. Strategic Manage.*, vol. 33, pp. 1–17, Sep. 2021.

[9] J. Gomes, S. Khan, and D. Svetinovic, "Fortifying the blockchain: A systematic review and classification of post-quantum consensus solutions for enhanced security and resilience," *IEEE Access*, vol. 11, pp. 74088–74100, 2023.

[10] M. A. Hannan, M. A. Shahriar, M. S. Ferdous, M. J. M. Chowdhury, and M. S. Rahman, "A systematic literature review of blockchain-based e-KYC systems," *Computing*, vol. 105, no. 10, pp. 2089–2118, Oct. 2023.

[11] P. K. Ozili, "Decentralized finance research and developments around the world," *J. Banking Financial Technol.*, vol. 6, no. 2, pp. 117–133, Oct. 2022.

[12] D. Berdik, S. Otoum, N. Schmidt, D. Porter, and Y. Jararweh, "A survey on blockchain for information systems management and security," *Inf. Process. Manage.*, vol. 58, no. 1, Jan. 2021, Art. no. 102397.

[13] S. Haber and W. S. Stornetta, "How to time-stamp a digital document," *J. Cryptol.*, vol. 3, no. 2, pp. 99–111, Jan. 1991.

[14] V. Kumar C and P. Selvaprabhu, "An examination of distributed and decentralized systems for trustworthy control of supply chains," *IEEE Access*, vol. 11, pp. 137025–137052, 2023.

[15] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Bus. Rev.*, vol. 4, no. 2, p. 15, Jan. 2008.

[16] M. M. Islam, Md. K. Islam, M. Shahjalal, M. Z. Chowdhury, and Y. M. Jang, "A low-cost cross-border payment system based on auditable cryptocurrency with consortium blockchain: Joint digital currency," *IEEE Trans. Services Comput.*, vol. 16, no. 3, pp. 1616–1629, May 2022.

[17] N. Kapsoulis, A. Psychas, G. Palaiokrassas, A. Marinakis, A. Litke, and T. Varvarigou, "Know your customer (KYC) implementation with smart contracts on a privacy-oriented decentralized architecture," *Future Internet*, vol. 12, no. 2, p. 41, Feb. 2020.

[18] B. D. S. Sai, R. Nikhil, S. Prasad, and N. S. Naik, "A decentralized KYC-based approach for microfinance using blockchain technology," *Cyber Secur. Appl.*, vol. 1, Dec. 2023, Art. no. 100009.

[19] R. Norvill, M. Steichen, W. M. Shbair, and R. State, "Demo: Blockchain for the simplification and automation of KYC result sharing," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, May 2019, pp. 9–10.

[20] N. Ullah, K. A. Al-Dhlan, and W. M. Al-Rahmi, "KYC optimization by blockchain based hyperledger fabric network," *Cyber Secur. Appl.*, vol. 1, pp. 1294–1299, Mar. 2021.

[21] B. Karadag, A. Halim Zaim, and A. Akbulut, "Blockchain-based KYC model for credit allocation in banking," *IEEE Access*, vol. 12, pp. 80176–80182, 2024.

[22] A. Thommandru and D. B. Chakka, "Recalibrating the banking sector with blockchain technology for effective anti-money laundering compliances by banks," *Sustain. Futures*, vol. 5, Dec. 2023, Art. no. 100107.

[23] A. K. Yadav and R. K. Bajpai, "KYC optimization using blockchain smart contract technology," *Int. J. Innov. Res. Appl. Sci. Eng.*, vol. 4, no. 3, pp. 669–674, Sep. 2020.

[24] N. Mansoor, K. F. Antora, P. Deb, T. A. Arman, A. A. Manaf, and M. Zareei, "A review of blockchain approaches for KYC," *IEEE Access*, vol. 11, pp. 121013–121042, 2023.

[25] P. Patil and M. Sangeetha, "Blockchain-based decentralized KYC verification framework for banks," *Proc. Comput. Sci.*, vol. 215, pp. 529–536, Jan. 2022.

[26] V. Schlatt, J. Sedlmeir, S. Feulner, and N. Urbach, "Designing a framework for digital KYC processes built on blockchain-based self-sovereign identity," *Inf. Manage.*, vol. 59, no. 7, Nov. 2022, Art. no. 103553.

[27] D. George, A. Wani, and A. Bhatia, "A blockchain based solution to know your customer (KYC) dilemma," in *Proc. IEEE Int. Conf. Adv. Netw. Telecommun. Syst. (ANTS)*, Dec. 2019, pp. 1–6.

C. VINOTH KUMAR received the master's degree in communication engineering from the PSG College of Technology, Coimbatore, Tamil Nadu, India, in 2012. He is currently pursuing the Ph.D. degree with the Electronics and Communication Engineering Department, Vellore Institute of Technology, Vellore, Tamil Nadu, India. He has also participated in various conferences, such as the International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN 2019) and the International Conference on Microelectronic Devices, Circuits and Systems (ICMDCS), organized by Vellore Institute of Technology. His research interests include blockchain and wireless communications.

POONGUNDRAN SELVAPRABHU received the bachelor's degree in electronics and communication engineering from Anna University, India, in 2009, the master's degree in electronics design from Mid Sweden University, Sweden, in 2012, and the Ph.D. degree in wireless and mobile communications from Chonbuk National University, Republic of Korea, in 2017. He was a Postdoctoral Research Fellow with the Division of Electronics and Information Engineering, Chonbuk National University, and Inha University, Republic of Korea, from 2017 to 2018. He is currently an Associate Professor with Vellore Institute of Technology, Vellore, Tamil Nadu, India. He was a participant in many projects, such as Brain Korea-21 (BK-21), World Class University (WCU), and the Ministry of Education Science and Technology (MEST) Project, which was funded by NRF, Republic of Korea. His main research interests include 5G wireless communications topics, especially interference alignment for massive MIMO, signal processing, information theory, NOMA, and wireless body area network (WBAN), with a focus on developing algorithms that optimize energy usage and ensure data security by leveraging blockchain technology.

NIVETHA BASKAR received the bachelor's degree in electronics and communication engineering and the master's degree in applied electronics from Anna University, India, in 2018 and 2020, respectively. She is currently pursuing the Ph.D. degree with the Electronics and Communication Engineering Department, Vellore Institute of Technology (VIT), Vellore, Tamil Nadu, India. She is a Research Scholar with the Electronics and Communication Engineering Department, VIT. Her research interests include wireless communications, 5G communication systems, massive MIMO, resource allocation, interference management, the IoT, and physical layer security.

U. VIVEK MENON received the master's degree in communication engineering from Vellore Institute of Technology, Vellore, Tamil Nadu, India, in 2019, where he is currently pursuing the Ph.D. degree with the Department of Electronics and Communication Engineering. He has participated in various conferences, such as the International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN 2019) and the International Conference on Microelectronic Devices, Circuits and Systems (ICMDCS), organized by Vellore Institute of Technology. His main research interests include interference alignment in wireless communication systems, interference management techniques in 5G cellular communication systems, massive MIMO, and the Internet of Things.

VINOTH BABU KUMARAVELU (Senior Member, IEEE) received the M.Tech. degree in communication engineering and the Ph.D. degree in MIMO-OFDM-based wireless communication from Vellore Institute of Technology, Vellore, Tamil Nadu, India, in 2009 and 2014, respectively. He is currently a Professor with the Department of Communication Engineering, School of Electronics Engineering, Vellore Institute of Technology. He works on spatial modulation, reconfigurable intelligent surfaces, non-orthogonal multiple access, wireless sensor networks, the Internet of Things, device-to-device communication, small cells, and vehicular ad hoc networks. He is the author of the books *Communication Engineering* and *Digital Communications*, published by Magnus Publications, India. His research interests include wireless communications, digital communications, and signal processing. During the M.Tech. degree, he won the Gold Medal. He was awarded merit scholarships twice during the master's degree with Vellore Institute of Technology for securing high grades.

SUNIL CHINNADURAI (Senior Member, IEEE) received the B.E. degree from Anna University, India, in 2009, the M.S. degree in electronics and communication engineering from Mid Sweden University, Sweden, in 2012, and the Ph.D. degree in electronics and communication engineering from Jeonbuk National University, South Korea, in 2017. He worked as a Postdoctoral Research Fellow at Jeonbuk National university for six months. He was with the signal intelligence research center, Hanyang University, Seoul, South Korea, for a year working as a Postdoctoral Research Scientist. He is currently working as an Associate Professor for the Department of ECE, SRM University AP, Andhra Pradesh, India, since March 2019. His research interests include 5G and B5G communications, intelligent reflecting surfaces, massive MIMO, NOMA, mm wave communications, machine learning and hyperspectral image processing. He is a IETE Fellow. He received the Best Paper Award at the 24th MSPT International Symposium in 2016.

FARMAN ALI received the B.S. degree in computer science from the University of Peshawar, Pakistan, in 2011, the M.S. degree in computer science from Gyeongsang National University, South Korea, in 2015, and the Ph.D. degree in information and communication engineering from Inha University, South Korea, in 2018. He was a Postdoctoral Fellow with the UWB Wireless Communications Research Center, from September 2018 to August 2019. He is currently an Assistant Professor with the Department of Applied AI, Sungkyunkwan University, South Korea. He has registered over four patents and published more than 100 research papers in peer-reviewed international journals and conferences. His current research interests include sentiment analysis, social networking analysis, medical informatics, machine learning and AI, recommendation systems, data science, and applied fuzzy logic. He has been awarded with Outstanding Research Award (Excellence of Journal Publications 2017) and the President Choice of the Best Researcher Award during the Graduate Program at Inha University. In 2022 and 2023, each year he was presented among "Top 2% Scientists in the World" by Stanford University for his career achievements.