Kyc Using Smart Contract Over Blockchain

Shiven Singh[1], Viraj Garg[2], Dr. Sathyapriya Loganathan[3]

[1,2]Department. of Computer Science and Engineering, SRM Institute of Science and Technology, Kattankulathur-603 203, India
[3]Assistant Professor, SRM Institute of Science and Technology, Kattankulathur-603 203, India

Abstract
Know Your Customer (KYC) is a requirement for financial institutions to use identity, qualification and risk to identify customers when establishing a banking relationship. With the focus on security, the KYC process has become difficult and costly to complete for any customer. In this article, we propose a convenient, instant, secure and transparent banking system KYC certification platform through Inter Planetary File System (IPFS) and block-chain technology. The system allows customers to open an account at any bank, complete the KYC process there, generate hashes using the IPFS network, and distribute them to other banks using the legacy urine of block-chain technology. Using a private key, all banks/financial institutions can use the IPFS network to securely store and store customer information (e.g. KYC) if the customer wants to open another account with that bank/financial institution. Additionally, leveraging block-chain technology ensures immutability and transparency of KYC information, thereby increasing security and reducing the risk of fraud or misuse of information.

Storing hashed KYC data on the IPFS network ensures that important customer data remains transparent and accessible only to authorized users, thus maintaining confidentiality and compliance with data protection laws. In addition, the processes that this new system can easily adjust will increase efficiency in the banking sector, allowing companies to allocate resources more efficiently and focus on providing better customer service.

By sharing KYC credentials across multiple banks, customers benefit from a quicker and faster account opening process; When banks come voluntarily, it builds trust and reduces the risks associated with new customers. Overall, the integration of block-chain and IPFS technology into the KYC process should transform the banking industry by providing efficient, secure and transparent solutions that enable customer satisfaction and compliance.

Keywords: Block-chain, KYC, Interplanetary File System, Security

I. Introduction

In the past two decades, technology has transformed how news content is created and delivered in the entertainment ands media sectors. Yet, challenges persist, particularly in the distribution of digital content and fair compensation for participants. A recent innovation explores using blockchain and cryptocurrencies to facilitate micropayments, allowing users to make small transactions for specific actions.

Blockchain and cryptocurrencies offer secure, private, low-fee transactions without intermediaries. They've birthed major cryptocurrencies like Bitcoin and Ethereum, driving interest in alternative cryptocurrencies (AltCoins) and financial concepts like Initial Coin Offerings (ICOs). Beyond cryptocurrencies, blockchain's distributed ledger technology (DLT) promises enhanced security and transparency, reducing reliance on laborious processes like Proof of Work (PoW).

Platforms like R3/Corda and Hyperledger Fabric support permissioned blockchains with high transaction speeds, attracting financial institutions seeking solutions to longstanding challenges like credit scoring for loans. Additionally, KYC/KYB processes are evolving, demanding dynamic customer data management to combat cyber threats effectively.

Blockchain's impact extends beyond finance, with proposals for decentralized frameworks in sectors like insurance. However, sharing transaction data on traditional blockchains can be costly, leading to considerations like using the InterPlanetary File System (IPFS) for sharing information more efficiently.

In conclusion, block chain's evolution from Bitcoin's inception has spurred innovations across industries, from finance to media, promising streamlined processes and improved security, albeit with ongoing challenges like data sharing costs.

II. Literature Survey

Block chain[1]is renowned as a distributed system for information storage, yet its irreversible and transparent nature poses challenges regarding personal data and privacy. Due to the inability to modify data once stored, block chain is designed to safeguard user identities. A common application is using block chain solely for time stamping, offering the added advantage of measuring data volumes.

Decryption key in this approach can expose encrypted content, limiting data encryption flexibility. Privacy[6] principles must be meticulously addressed in blockchain transactions, especially concerning personal or sensitive information.

Blockchain[2] technology has evolved significantly, surpassing its initial application in cryptocurrencies like Bitcoin. Ethereum, in particular, has introduced smart contracts that revolutionize decentralized applications (DApps) by eliminating fraud and third- party intervention. These contracts operate using sophisticated programming languages, empowering users to create and deploy DApps and execute smart contracts seamlesly.

Research has explored blockchain's applications across various sectors, including government institutions, financial mechanisms, and justice systems. The integration of blockchain with Internet of Things (IoT) sensor data also holds promise for businesses seeking secure data sharing and monetization opportunities.

In the finance[10] and banking sectors, blockchain's potential is evident in facilitating peer-to-peer digital information exchange with minimal intermediaries. Additionally,[4] blockchain technology is being explored for KYC (Know Your Customer) processes to streamline customer identity verification and compliance procedures for financial institutions.

When a client wants to do the financial transaction through[3] a payment provider, they will check the customer identity by his name from Bank if the provided information is correct through Block- chain smart contract . The author[8] provided an assumption on using the blockchain to make the identity and financial transaction through blockchain, though they did not provide any use c ase for document sharing like KYC docs. A typical KYC framework could be that a client goes to a bank, the bank performs KYC, stores KYC in the Blockchain, give a customer a token and then customer give access to another bank to check the KYC information. The other bank then crosschecks the information from Blockchain. Because of a range of configuration parameters, the blockchain is somewhat uncontrollable. For example, test nets like Rinkby, Ethereum cannot be adjusted easily because of their parameters like Gas limit, Mining difficulty and so on. Authors[7] suggested using Grid'5000, as they found it highly controllable and configurable tested. Again, the authors did not provide a practical use case scenario with cost calculation. J. Parra Moyano et al.[13] has shown the design of centralized and decentralized Blockchain KYC solution with the division of processing cost among different banks. To minimize[11] the cost of core KYC[5] verification and improve the customer experience, they proposed a new scheme based on distributed ledger technology (DLT). They Focused on four main points. The first is proportionality: the cost will be shared proportionally by all the institutions involved with a particular KYC verification process.

They focused on Irrelevance secondly. The one who avoids the KYC process will not get any incentive. The third point of focus was Privacy. The KYC verification process has to be secured so that user privacy is not violated. Finally, they focused on No- minting[8]. [14]As the process is online-based, they need to focus that no false can be made during KYC verification.

Whenever[9] someone tries to edit any portion of KYC data, that editing process will automatically be void from the authoritative side.

III. Problem Statements

The aim is to reduce the cost of the KYC process by using block chain to solve the KYC cost issue for financial institutions. Currently, many third-party service providers and external verification bodies provide information and interventions to obtain the needed information from customers.

However, banks have difficulty collecting this information to obtain their customers' consent. This increased the number of times banks failed to comply with regulatory requirements, leading to large fines and reputation damage.

Therefore, before reviewing, the bank must digitize the information in the file and enter it into the warehouse. This is an extreme case as it uses advanced technology platforms.

KYC often faces new rules and regulations in many areas. Therefore, utilities need to adjust their aspects. This has increased the need for banks to improve their data collection processes to ensure effective and timely risk management.

Banks do not have a centralized or integrated KYC system for their various activities such as wealth management, asset management and banking. Therefore, managing many systems and integrating different issues causes a lot of pressure and costs on banks.

This article covers this issue from our perspective: First, all financial institutions in the same country must comply with the same KYC requirements and agree on the process of issuing important KYC certificates to customers.

Second, all financial institutions working with the system agree on the average cost of performing the important KYC verification process. This price may depend on each client's complexity (as determined in advance).

In addition, it should be noted that national regulatory authorities are instrumental in monitoring and managing these systems effectively. They strongly encourage financial institutions to actively engage and cooperate with the system, aiming to improve the efficiency and transparency of the KYC verification process. These three critical assumptions serve as foundational principles to guarantee the accurate setup and smooth operation of the relevant financial entities within the regulatory landscape.

IV. Objectives

When a client engages with two different banks, the process unfolds as follows: Initially, the client visits Bank A and submits their KYC (Know Your Customer) details for verification. Bank A adopts our proposed framework, providing the client with a hash value and verifying how the sender's hash aligns with the client's hash. Subsequently, Bank A shares the user's data with Bank B and Bank C, enabling swift verification of KYC information by both banks. Utilizing the IPFS (Inter Planetary File System) network, banks upload and store KYC data securely. However, prior to sharing KYC data on the IPFS network, encryption is applied to enhance security and minimize file size. Consequently, individuals can access KYC information from the IPFS network by referencing the hash value.

4.1 Requirement Analysis

The project aims to evaluate the design of different applications to enhance their usability. An essential aspect for customer satisfaction is optimizing navigation between screens to ensure efficiency and minimizing user input. Furthermore, selecting a browser version that is compatible with a wide range of browsers will enhance the accessibility of the app.

V. Proposed Methodology

Figure 1 illustrates the repetitive process that occurs when a customer interacts with three different financial institutions. Although the fundamental procedure remains the same, each instance displays evidence values thrice. It's crucial to note that the "basic" process denotes the minimum KYC verification required by all legitimate financial entities.

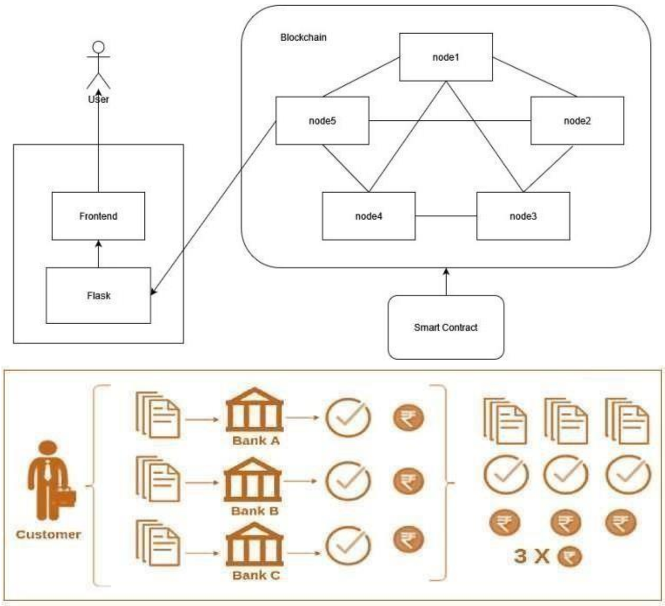


Figure 1. Current KYC Verification Process

Block chain is an integrated online transaction system that enables direct peer-to-peer money transfers without relying on traditional financial intermediaries. Changes and transactions are recorded and validated through a proof-of-work mechanism, with each validated transaction forming a block in the block chain. This decentralized system, exemplified by Bitcoin, ensures secure and transparent transactions across the Internet. Moreover, Distributed Ledger Technology (DLT) goes beyond cryptocurrency creation to enable online data verification and sharing through smart contracts. These contracts facilitate secure and automated interactions, especially in sectors dealing with luxury goods and digital assets.

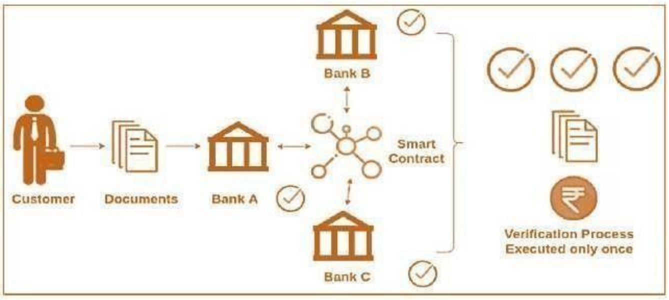


Figure 2. KYC Verification Process after implementation of block chain

The Interplanetary File System is a peer-to-peer hypermedia protocol, which connects computing devices for sharing/storing files/data. The content in the file is distinctively recognized in the global name space using the hash code of the file. If the hash If the numbers are different, the file cannot be identified and will be recognized by IPFS. Additionally, IPFS recognizes parity if files with identical content are stored.

5.1 KYC Verification

Consider a scenario where a customer seeks to open an account at Bank A. The customer transmits account details and KYC information to the bank, which thoroughly analyzes the messages for accuracy. Upon verification, the data is encrypted using the bank's application system, enabling seamless sharing with other banking institutions and maintaining a local backup.

Bank A securely stores the encrypted data on its private IPFS network and uploads the corresponding hash value to the block chain network. Additionally, a copy of the KYC information is retained in the bank's local database.

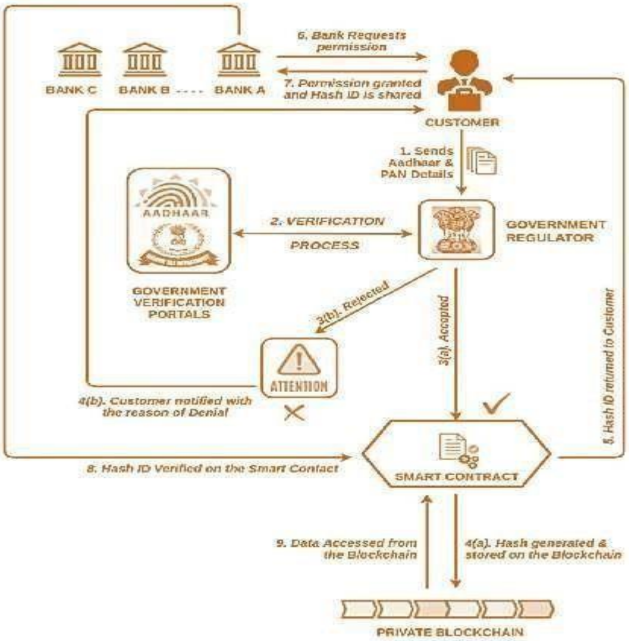

BANK C
BANK B ----
BANK A
6. Bank Requests permission
7. Permission granted and Hash ID is shared
CUSTOMER
1. Sends Aadhaar & PAN Details
AADHAAR
2. VERIFICATION PROCESS
GOVERNMENT REGULATOR
GOVERNMENT VERIFICATION PORTALS
3(b). Rejected
3(a). Accepted
5. Hash ID returned to Customer
ATTENTION
4(b). Customer notified with the reason of Denial
8. Hash ID Verified on the Smart Contact
SMART CONTRACT
9. Data Accessed from the Blockchain
4(a). Hash generated & stored on the Blockchain
PRIVATE BLOCKCHAIN

Figure 3 depicts the workflow of this proposed system.

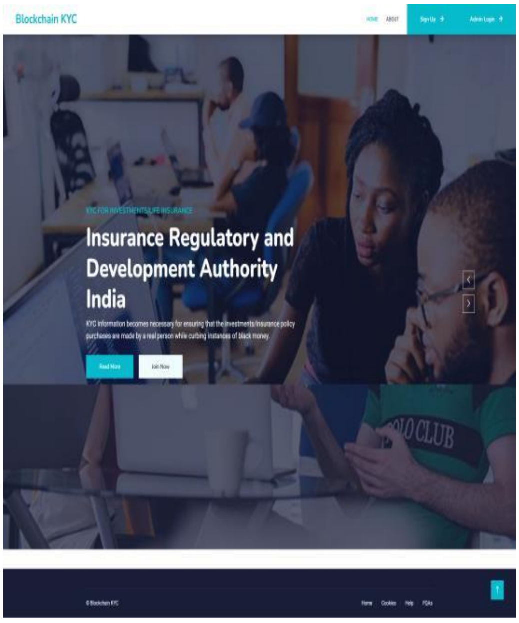
Bank A then shares the block-chain and IPFS hash results with the customer, allowing them to grant access to the KYC package by sharing the hash with other institutions as needed. Subsequently, if the customer decides to open an account at Bank B, they will share the IPFS hash value with Bank B.

Bank B, having permission to access the hash from the customer, retrieves the desired hash value from the block chain network. Using this hash value, Bank B downloads the encrypted KYC data from the IPFS network and stores it securely, alongside a local copy of the information, using the customer's private key. The regulatory authority overseeing these operations is defined as the central bank.

5.2 Result

The application boasts a user-friendly web interface that enables users to upload documents and monitor their verification status. Additionally, it empowers administrators to manage both users and their documents efficiently.

5.2.1



Insurance Regulatory and Development Authority India

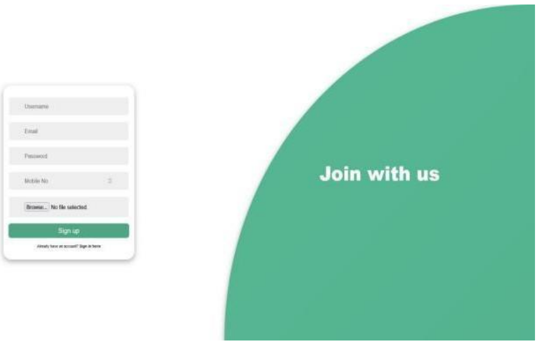
KYC information becomes necessary for ensuring that the investments/insurance policy purchases are made by a real person while curbing instances of black money.

Front Page

The initial page of the KYC verification app acts as a gateway to the application's features. It presents two options for users: sign up and login, accessible via corresponding buttons. To use the document uploading and verification functionalities, users must first log in. These pages are kept inaccessible until login to protect users' sensitive KYC data from unauthorized access.

5.2.2

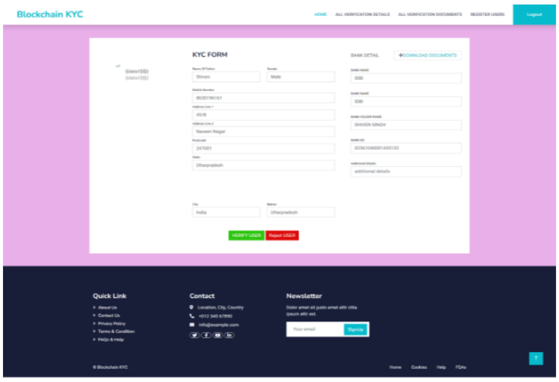
Sign Up (register)



Clicking on the "Sign Up" button grants access to the registration form, prompting users to provide basic details like name, email, and password. Upon successful registration, users are directed to the login page to enter credentials for accessing KYC verification features. Once logged in, users can upload and verify KYC documents, including a government ID, proof of address, and a selfie for facial recognition. The app automates document validation and identity verification through facial recognition. If automatic verification fails, documents are reviewed manually by an expert to ensure accuracy. The app's user-friendly interface includes a dashboard for real-time verification updates, enhancing transparency and efficiency.

5.2.3

KYC form



KYC FORM

Name Of Father: Shiven
Gender: Male
Mobile Number: 8630196161
Address Line 1: 45/8
Address Line 2: Naveen Nagar
Postcode: 247001
State: Uttarpradesh
City: India
Nation: Uttarpradesh

BANK DETAIL

BANK NAME: IDBI
BANK NAME: IDBI
BANK HOLDER NAME: SHIVEN SINGH
BANK NO: 0236104000014335132
Additional Details: additional details

In the KYC Form section, there are fields for the name of the father, gender, mobile number, address, postcode, state, city, and nation. The information filled out suggests that the individual is male, named Shiven, and resides in Uttar Pradesh, India.

The Bank Detail section includes fields for the bank name, bank holder name, and bank account number, with the bank name being IDBI and the account holder's name being Shiven Singh. There is also a button to download documents, which might be used to obtain additional verification documents provided by the user.

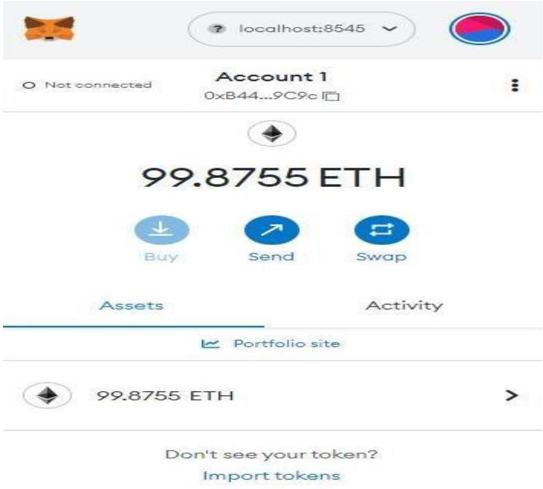
At the bottom of the form, there are two action buttons: "VERIFY USER" and "Reject USER," which are likely used by an administrator or automated system to either approve or reject the KYC submission after reviewing the provided information.

The footer of the web page contains quick links to various sections like About Us, Contact Us, Privacy Policy, Terms & Condition, FAQs & Help, and a contact section with a phone number and email address placeholder. There's also a section for a newsletter subscription.

The overall design and layout suggest that this is an administrative interface for processing KYC applications, possibly for a financial or blockchain-related service where identity verification is required.

5.2.5

Meta Mask



Not connected
Account 1
0xB44...9C9c
99.8755 ETH
99.8755 ETH
Don't see your token?

VI. Conclusion

The current document verification process involves numerous manual steps, such as submitting physical documents, making copies, and meticulously verifying their authenticity. These procedures can be extremely time- consuming, and the inherent risk of human error often leads to significant delays in the verification process. However, by harnessing the power of new and innovative technologies like block chain, we have the opportunity to revolutionize these cumbersome processes and streamline verification tasks, resulting in substantial time and cost savings.

Block chain technology offers a secure and tamper-proof method of storing and verifying data, making it an ideal solution for enhancing the document verification process. Each document can be represented as a unique digital asset on the block chain, and its authenticity and integrity can be easily verified through the block chain's robust consensus mechanism. This not only ensures a high level of trust and transparency but also significantly reduces the likelihood of data manipulation or unauthorized alterations.

In addition to these benefits, a block chain-based document verification system can also lead to considerable cost reductions. By eliminating the need for intermediaries and manual intervention, organizations can significantly decrease verification. This is particularly advantageous in industries such as finance, where stringent regulatory compliance requirements necessitate thorough document verification processes.

Furthermore, adopting a block chain-based approach to document verification can also enhance data privacy and security. Traditional verification methods often involve sharing sensitive information with multiple entities, increasing the risk of data breaches and privacy infringements. However, by leveraging block-chain technology, companies can ensure that data is securely stored and accessible only to authorized parties, mitigating the risk of unauthorized access and bolstering overall data security.

In conclusion, leveraging block chain technology for document verification not only streamlines processes, reduces costs, and enhances data privacy and security but also introduces a paradigm shift towards a more efficient and trustworthy verification ecosystem. Embracing these innovations can lead to transformation advancements across various industries, revolutionizing how organizations manage and verify critical documents with unparalleled reliability and security measures in place.

REFERENCES

1. *F. Glaser*, “Pervasive Decentralization of Digital Infrastructures: A Framework for Block-chain Enabled System and Use Case Analysis,” Social Science Research Network, Rochester, NY, SSRN Scholarly Paper ID 3052165, Jan. 2017.
2. *A. Rahman, S. Roy, M. S. Kaiser, and M. S. Islam*, “A lightweight multi-tier s-mqtt framework to secure communication between low-end ioi nodes,” in 2016 5th International Conference
3. *M. Raikwar, S. Mazumdar, S. Ruj, S. Sengupta, A.Chattopadhyay, and K.-Y. Lain*, “A Blockchain Framework for Insurance Process Conference on New Technologies, Mobility and Security (NTMS), 2018.
4. *Puthal, N. Malik, S. Mohanty, E. Kougianos, and C. Yang*, “The Blockchain as a Decentralized Security Framework [FutureDirections],” IEEE Consumer Electronics Magazine, scd. 7, pp. 18—21, 2018.
5. *Rahman, M. A. Rahman, A. Shabut, S. AlMamun, and A. Hussain*, “A Brain-Inspired Trust Management Model to Assure Security in a Cloud Based IoT Framework for Neuroscience

Applications,"

6. *Abdullah Al Mamun, Sheikh Riad Has, Md Salahuddin Bhuiyan, M.Shamim Kaiser and Mohammad Abu Yousuf*, "Secure and Transparent KYC for Banking System Using IPFS and Block-chain Technology", 2020 IEEE Region 10 Symposium the operational expenses associated with document
7. *Nikita Singhal, Mohit Kumar Sharma, Sandeep Singh Samant, Prajwal Goswami and Y.Abhilash Reddy*, "Smart KYC Using Blockchain and IPFS", Springer Nature Singapore Pte Ltd. 2020
8. *Dr. Manoj Kumar, Nikhil, Parina Anand*, "A Block-chain Based Approach For An Efficient Secure KYC Process With Data Sovereignty ", International Journal Of Scientific & Technology Research Volume 9, Issue 01, January 2020
9. *Liu, J. and Zhen-Tian Liu*. "A Survey on Security Verification of Block-chain Smart Contracts." IEEE Access 7 (2019): 77894-77904.
10. Avoid attacks in WSN for IoT Devices," 2019 International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2019, pp. 1898-1901
11. *Dr.R.Chinnaiyan , M.S.Nidhya* (2018), " Reliability Evaluation of Wireless Sensor Networks using EERN Algorithm" , Lecture Notes on Data Engineering and Communications Technologies, Springer International conference on Computer Networks and Inventive Communication Technologies (ICCNCT - 2018), August 2018 (Online)
12. *Md. Abdul Hannan, Md. Atik Shahriar, "*A systematic literature review of blockchain-based e-KYC system
13. *Rosati, P.; Cuk, T.* Block-chain Beyond Cryptocurrencies: FinTech and Strategy in the 21st Century. In Disrupting Finance, Lynn, T., Mooney, J.G., Rosati, P., Cummins, M. (Eds.), pp.149-170, 2016.
14. *Divya. R and Dr.R. Chinnaiyan*, "Reliable Constrained Application Protocol to Sense and *Dr.R.Chinnaiyan, Abishek Kumar* (2017) " Reliability Assessment of Component Based Software Systems using Basis Path Testing" .