**ENABLING TRUST AND PRIVACY-PRESERVING E-KYC SYSTEM USING BLOCKCHAI**

**ABSTRACT:**

The electronic know your customer (e-KYC) is a system for the banking or identity provider to establish a customer identity data verification process between relying parties. Due to the efficient resource consumption and the high degree of accessibility and availability of cloud computing, most banks implement their e-KYC system on the cloud. Essentially, the security and privacy of e-KYC related documents stored in the cloud becomes the crucial issue. Existing e-KYC platforms generally rely on strong authentication and apply traditional encryption to support their security and privacy requirement. In this model, the KYC system owner encrypts the file with their host’s key and uploads it to the cloud. This method induces encryption dependency and communication and key management overheads. In this paper, we introduce a novel blockchain-based e-KYC scheme called e-KYC TrustBlock based on the ciphertext policy attributebased encryption (CP-ABE) method binding with the client consent enforcement to deliver trust, security and privacy compliance. In addition, we introduce attribute-based encryption to enable the privacy preserving and fine-grained access of sensitive transactions stored in the blockchain. Finally, we conduct experiments to show that our system is efficient and scalable in practice.

**INTRODUCTION:**

Electronic-Know Your customer (e-KYC) is a service that banks or financial institutions (FIs) provide virtual banking operation related to authentication and verification of identity electronically to their customers for improving cost efficiency and customer satisfaction. The e-KYC system enables FIs to electronically verify their customer identity and retrieve KYC data for both individual and corporate clients. To implement the e-KYC system, financial institutions either employ offthe-shelf e-KYC software fully equipped with necessary functions or develop their own. Then, they can deploy the system as an on-premise or a cloud-based model. Due to the trend of the outsourcing model, most enterprises have adopted the cloud as the preferred platform for housing their system and data. A cloud-based e-KYC system provides a more efficient and flexible authentication method compared to the hostbased e-KYC authentication method where documents need to be validated via the centralized host. This causes a traffic bottleneck and single point of failure problem. Also, the traceability of the verified transaction is limited since all transactions occurring in the system are entirely managed by the provider. Nevertheless, the security and privacy issue of a cloud-based solution is a concern for many potential enterprises. This is because e-KYC system located on the cloud store customer data documents and it might be viewed by any public cloud tenants or even the cloud service providers (CSPs). To address this concern, most banks and FIs need to implement an encryption mechanism in addition to the strong authentication feature provided by the CSPs. To this end, banks and FIs possessing the e-KYC system need to encrypt the e-KYC data files before they are uploaded to the cloud. When the relying parties request for verification, the host party can either perform the verification by either decrypting the file and sending back the confirmation of the verification result to the requestor or transmitting the copy of encrypted files along with the decryption key to the requestor. This first approach introduces the overheads related to the verification process, communication, and centralized decryption while the latter approach needs to handle key management especially secure key sharing. Specifically, key revocation and key re-generation in the cloud e-KYC environment have not been addressed by any research works. If the client would like to withdraw his consent from any banks or FIs, they have no right to store the client’s identity data anymore. Accordingly, the data should be completely deleted and the decryption key needs to be revoked. Any banks or FIs sharing the revoked key need to regenerate a key to fully guarantee that unauthorized banks or FIs cannot access the client’s data stored in the cloud. In addition to the aforementioned problems, exiting cloud e-KYC platforms do not provide shared information for the transaction occurring in the e-KYC verification available for traceability. Recently, blockchain technology has attracted huge interest by a number of enterprises in many industries including the banking and financial sector. There is a growing interest in using e-KYC platforms that use blockchain and cloud system. Blockchain technology truly promotes the decentralized system enabling transparency, agility, trustworthiness, and costeffectiveness for transaction processing and management in multi-user and multi-provider environment. In the blockchain system, a smart contract which is a self-executing program that can be implemented on the blockchain enables the automated execution of system logics or functions efficiently. This empowers the usability and programmability of any systems running on the blockchain network. For years, a number of research works related to blockchain-based KYC have proposed to deliver the decentralized authentication and verification process. However, there are shortcomings that have not been fully solved by existing works. First, there are no works that provide electronic client’s consent function with the solid nonrepudiation property which is an essential requirement of privacy regulations such as General Data Protection Act (GDPR) [18] in the KYC registration process. Second, most existing works overlook the privacy of transaction stored in the smart contract and blockchain. In addition to the identity or credential documents that are encrypted on the cloud storage, the privacy of all e-KYC processing transactions such as transaction status sharing, data origin authentication, and smart contract that contains personal data stored in the blockchain should be preserved. Finally, most works have a limited feature to allow the customers to access and update their credentials located on the cloud service paid by the FI. In this paper, we aim to address such research gaps by introducing a secure and efficient blockchain-based eKYC documents registration and verification process with lightweight key cryptographic protocols run in the cloud Interplanetary File System (IPFS). To facilitate the foundational privacy requirement regarding the user’s consent collection, we develop a smart contract to generate and enforce the consent to be digitally signed by the customer. The consents will be systematically stored in a blockchain having tamper-proof property which is useful for auditing. Regarding the data privacy issue, we propose an optimized cryptographic protocol by applying symmetric encryption with public key encryption to encrypt the customers’ credential files and employ the ciphertext policy attribute-based encryption (CP-ABE) to encrypt the blockchain transactions. Since CP-ABE provides a one-to-many encryption with fine-grained access control, it allows several FIs to access common encrypted transactional data in the blockchain of the same client based on the access policy defined. Specifically, we devise the policy update algorithm to enable efficient reencryption based on a less complicated policy tree structure. Finally, our system allows users to update their e-KYC data with any banks or FIs engaging in the blockchain. The updated e-KYC data is broadcasted in the ledger and the synchronization of the updated data is done by the responsible smart contract. This paper is structured as follows. Section 2 presents related works. Section 3 explains the theoretical background used in our proposed approach. Section 4 presents our proposed system model. Section 5 provides the security analysis of our scheme. Section 6 provides the evaluation analysis and experiments. Section 7 gives conclusion and future work.

**EXISTING SYSTEM**

A cloud-based e-KYC system provides a more efficient and flexible authentication method compared to the hostbased e-KYC authentication method where documents need to be validated via the centralized host. This causes a traffic bottleneck and single point of failure problem. Also, the traceability of the verified transaction is limited since all transactions occurring in the system are entirely managed by the provider. Nevertheless, the security and privacy issue of a cloud-based solution is a concern for many potential enterprises. This is because e-KYC system located on the cloud store customer data documents and it might be viewed by any public cloud tenants or even the cloud service providers (CSPs). blockchain technology has attracted huge interest by a number of enterprises in many industries including the banking and financial sector. There is a growing interest in using e-KYC platforms that use blockchain and cloud system. Blockchain technology truly promotes the decentralized system enabling transparency, agility, trustworthiness, and costeffectiveness for transaction processing and management in multi-user and multi-provider environment. In the blockchain system, a smart contract which is a self-executing program that can be implemented on the blockchain enables the automated execution of system logics or functions efficiently. This empowers the usability and programmability of any systems running on the blockchain network. For years, a number of research works related to blockchain-based KYC have proposed to deliver the decentralized authentication and verification process. However, there are shortcomings that have not been fully solved by existing works. First, there are no works that provide electronic client’s consent function with the solid nonrepudiation property which is an essential requirement of privacy regulations such as General Data Protection Act (GDPR) [18] in the KYC registration process. Second, most existing works overlook the privacy of transaction stored in the smart contract and blockchain. In addition to the identity or credential documents that are encrypted on the cloud storage, the privacy of all e-KYC processing transactions such as transaction status sharing, data origin authentication, and smart contract that contains personal data stored in the blockchain should be preserved. Finally, most works have a limited feature to allow the customers to access and update their credentials located on the cloud service paid by the FI.

**PROPOSED SYSTEM**

we aim to address such research gaps by introducing a secure and efficient blockchain-based e KYC documents registration and verification process with lightweight key cryptographic protocols run in the cloud Interplanetary File System (IPFS). To facilitate the foun dational privacy requirement regarding the user’s consent collection, we develop a smart contract to generate and enforce the consent to be digitally signed by the customer. The consents will be systematically stored in a blockchain having tamper-proof property which is useful for auditing. Regarding the data privacy issue, we propose an optimized cryptographic protocol by applying symmetric encryption with public key encryption to encrypt the customers’ credential files and employ the ciphertext policy attribute-based encryption (CP-ABE) to encrypt the blockchain transactions. Since CP-ABE provides a one-to-many encryption with fine-grained access control, it allows several FIs to access common encrypted transactional data in the blockchain of the same client based on the access policy defined. Specifically, we devise the policy update algorithm to enable efficient re-encryption based on a less complicated policy tree structure. Finally, our system allows users to update their e-KYC data with any banks or FIs engaging in the blockchain. The updated e-KYC data is broadcasted in the ledger and the synchronization of the updated data is done by the responsible smart contract.

**SYSTEM STUDIES**

An important outcome of preliminary investigation is the determination that the system request is feasible. This is possible only if it is feasible within limited resource and time. The different feasibilities that have to be analyzed are

• OPERATIONAL FEASIBILITY

• ECONOMIC FEASIBILITY

• TECHNICAL FEASIBILITY

**Operational Feasibility**

Operational Feasibility deals with the study of prospects of the system to be developed. This system operationally eliminates all the tensions of the Admin and helps him in effectively tracking the project progress. This kind of automation will surely reduce the time and energy, which previously consumed in manual work. Based on the study, the system is proved to be operationally feasible.

**Economic Feasibility**

Economic Feasibility or Cost-benefit is an assessment of the economic justification for a computer based project. As hardware was installed from the beginning & for lots of purposes thus the cost on project of hardware is low. Since the system is a network based, any number of employees connected to the LAN within that organization can use this tool from at any time. The Virtual Private Network is to be developed using the existing resources of the organization. So the project is economically feasible.

**Technical Feasibility**

According to Roger S. Pressman, Technical Feasibility is the assessment of the technical resources of the organization. The organization needs IBM compatible machines with a graphical web browser connected to the Internet and Intranet. The system is developed for platform Independet environment. Java Server Pages, JavaScript, HTML, SQL server and Web Logic Server are used to develop the system. The technical feasibility has been carried out. The system is technically feasible for development and can be developed with the existing.

**INPUT DESIGN**

Input Design plays a vital role in the life cycle of software development, it requires very careful attention of developers. The input design is to feed data to the application as accurate as possible. So inputs are supposed to be designed effectively so that the errors occurring while feeding are minimized. According to Software Engineering Concepts, the input forms or screens are designed to provide to have a validation control over the input limit, range and other related validations.

This system has input screens in almost all the modules. Error messages are developed to alert the user whenever he commits some mistakes and guides him in the right way so that invalid entries are not made. Let us see deeply about this under module design.

Input design is the process of converting the user created input into a computer-based format. The goal of the input design is to make the data entry logical and free from errors. The error is in the input are controlled by the input design. The application has been developed in user-friendly manner. The forms have been designed in such a way during the processing the cursor is placed in the position where must be entered. The user is also provided within an option to select an appropriate input from various alternatives related to the field in certain cases.

Validations are required for each data entered. Whenever a user enters an erroneous data, error message is displayed and the user can move on to the subsequent pages after completing all the entries in the current page.

**OUTPUT DESIGN**

The Output from the computer is required to mainly create an efficient method of communication within the company primarily among the project leader and his team members, in other words, the administrator and the clients. The output of VPN is the system which allows the project leader to manage his clients in terms of creating new clients and assigning new projects to them, maintaining a record of the project validity and providing folder level access to each client on the user side depending on the projects allotted to him. After completion of a project, a new project may be assigned to the client. User authentication procedures are maintained at the initial stages itself. A new user may be created by the administrator himself or a user can himself register as a new user but the task of assigning projects and validating a new use rests with the administrator only.The application starts running when it is executed for the first time. The server has to be started and then the internet explorer in used as the browser. The project will run on the local area network so the server machine will serve as the administrator while the other connected systems can act as the clients. The developed system is highly user friendly and can be easily understood by anyone using it even for the first time.

**SOFTWARE ENVIRONMENT**

**Java Technology**

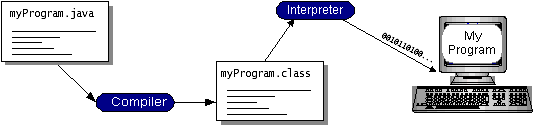
Java technology is both a programming language and a platform.

**The Java Programming Language**

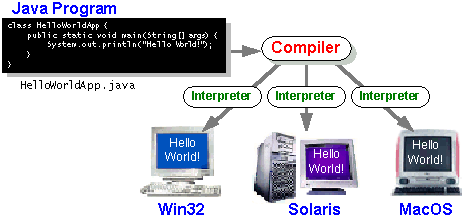
The Java programming language is a high-level language that can be characterized by all of the following buzzwords:

* + - Simple
    - Architecture neutral
    - Object oriented
    - Portable
    - Distributed
    - High performance
    - Interpreted
    - Multithreaded
    - Robust
    - Dynamic
    - Secure

With most programming languages, you either compile or interpret a program so that you can run it on your computer. The Java programming language is unusual in that a program is both compiled and interpreted. With the compiler, first you translate a program into an intermediate language called *Java byte codes* —the platform-independent codes interpreted by the interpreter on the Java platform. The interpreter parses and runs each Java byte code instruction on the computer. Compilation happens just once; interpretation occurs each time the program is executed. The following figure illustrates how this works.



You can think of Java byte codes as the machine code instructions for the *Java Virtual Machine* (Java VM). Every Java interpreter, whether it’s a development tool or a Web browser that can run applets, is an implementation of the Java VM. Java byte codes help make “write once, run anywhere” possible. You can compile your program into byte codes on any platform that has a Java compiler. The byte codes can then be run on any implementation of the Java VM. That means that as long as a computer has a Java VM, the same program written in the Java programming language can run on Windows 2000, a Solaris workstation, or on an iMac.



**6.2 Java Platform**

A *platform* is the hardware or software environment in which a program runs. We’ve already mentioned some of the most popular platforms like Windows 2000, Linux, Solaris, and MacOS. Most platforms can be described as a combination of the operating system and hardware. The Java platform differs from most other platforms in that it’s a software-only platform that runs on top of other hardware-based platforms.

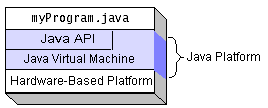
The Java platform has two components:

* The *Java Virtual Machine* (Java VM)
* The *Java Application Programming Interface* (Java API)

You’ve already been introduced to the Java VM. It’s the base for the Java platform and is ported onto various hardware-based platforms.

The Java API is a large collection of ready-made software components that provide many useful capabilities, such as graphical user interface (GUI) widgets. The Java API is grouped into libraries of related classes and interfaces; these libraries are known as *packages*. The next section what Can Java Technology Do? Highlights what functionality some of the packages in the Java API provide.

The following figure depicts a program that’s running on the Java platform. As the figure shows, the Java API and the virtual machine insulate the program from the hardware.



Native code is code that after you compile it, the compiled code runs on a specific hardware platform. As a platform-independent environment, the Java platform can be a bit slower than native code. However, smart compilers, well-tuned interpreters, and just-in-time byte code compilers can bring performance close to that of native code without threatening portability.

**What Can Java Technology Do?**

The most common types of programs written in the Java programming language are *applets* and *applications*. If you’ve surfed the Web, you’re probably already familiar with applets. An apple is a program that adheres to certain conventions that allow it to run within a Java-enabled browser.

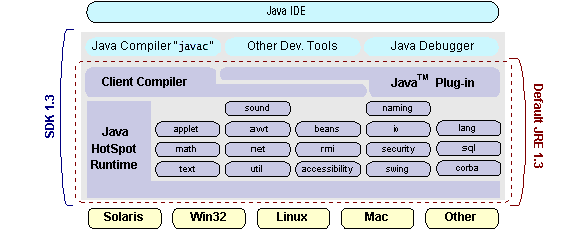
However, the Java programming language is not just for writing cute, entertaining applets for the Web. The general-purpose, high-level Java programming language is also a powerful software platform. Using the generous API, you can write many types of programs.

An application is a standalone program that runs directly on the Java platform. A special kind of application known as a *server* serves and supports clients on a network. Examples of servers are Web Servlets proxy servers, mail servers, and print servers. Another specialized program is a *servlet* A servlets can almost be thought of as an applet that runs on the server side. Java Servlets are a popular choice for building interactive web applications, replacing the use of CGI scripts. Servlets are similar to applets in that they are runtime extensions of applications. Instead of working in browsers, though, serviettes run within Java Web servers, configuring or tailoring the server.

How does the API support all these kinds of programs? It does so with packages of software components that provides a wide range of functionality. Every full implementation of the Java platform gives you the following features:

* **The essentials**: Objects, strings, threads, numbers, input and output, data structures, system properties, date and time, and so on.
* **Applets**: The set of conventions used by applets.
* **Networking**: URLs, TCP (Transmission Control Protocol), UDP (User Data gram Protocol) sockets, and IP (Internet Protocol) addresses.
* **Internationalization**: Help for writing programs that can be localized for users worldwide. Programs can automatically adapt to specific locales and be displayed in the appropriate language.
* **Security**: Both low level and high level, including electronic signatures, public and private key management, access control, and certificates.
* **Software components**: Known as JavaBeans can plug into existing component architectures.
* **Object serialization**: Allows lightweight persistence and communication via Remote Method Invocation (RMI).
* **Java Database Connectivity (JDBCTM)**: Provides uniform access to a wide range of relational databases.

The Java platform also has APIs for 2D and 3D graphics, accessibility, servers, collaboration, telephony, speech, animation, and more. The following figure depicts what is included in the Java 2 SDK.



**How Will Java Technology Change My Life*?***

We can’t promise you fame, fortune, or even a job if you learn the Java programming language. Still, it is likely to make your programs better and requires less effort than other languages. We believe that Java technology will help you do the following:

* **Get started quickly**: Although the Java programming language is a powerful object-oriented language, it’s easy to learn, especially for programmers already familiar with C or C++.
* **Write less code**: Comparisons of program metrics (class counts, method counts, and so on) suggest that a program written in the Java programming language can be four times smaller than the same program in C++.
* **Write better code**: The Java programming language encourages good coding practices, and its garbage collection helps you avoid memory leaks. Its object orientation, its JavaBeans component architecture, and its wide-ranging, easily extendible API let you reuse other people’s tested code and introduce fewer bugs.
* **Develop programs more quickly**: Your development time may be as much as twice as fast versus writing the same program in C++. Why? You write fewer lines of code and it is a simpler programming language than C++.
* **Avoid platform dependencies with 100% Pure Java**: You can keep your program portable by avoiding the use of libraries written in other languages. The 100% Pure Java Product Certification Program has a repository of historical process manuals, white papers, brochures, and similar materials online.
* **Write once, run anywhere**: Because 100% Pure Java programs are compiled into machine-independent byte codes, they run consistently on any Java platform.
* **Distribute software more easily**: You can upgrade applets easily from a central server. Applets take advantage of the feature of allowing new classes to be loaded “on the fly,” without recompiling the entire program.

**ODBC**

Microsoft Open Database Connectivity (ODBC) is a standard programming interface for application developers and database systems providers. Before ODBC became a *de facto* standard for Windows programs to interface with database systems, programmers had to use proprietary languages for each database they wanted to connect to. Now, ODBC has made the choice of the database system almost irrelevant from a coding perspective, which is as it should be. Application developers have much more important things to worry about than the syntax that is needed to port their program from one database to another when business needs suddenly change.

Through the ODBC Administrator in Control Panel, you can specify the particular database that is associated with a data source that an ODBC application program is written to use. Think of an ODBC data source as a door with a name on it. Each door will lead you to a particular database. For example, the data source named Sales Figures might be a SQL Server database, whereas the Accounts Payable data source could refer to an Access database. The physical database referred to by a data source can reside anywhere on the LAN.

The ODBC system files are not installed on your system by Windows 95. Rather, they are installed when you setup a separate database application, such as SQL Server Client or Visual Basic 4.0. When the ODBC icon is installed in Control Panel, it uses a file called ODBCINST.DLL. It is also possible to administer your ODBC data sources through a stand-alone program called ODBCADM.EXE. There is a 16-bit and a 32-bit version of this program and each maintains a separate list of ODBC data sources.

From a programming perspective, the beauty of ODBC is that the application can be written to use the same set of function calls to interface with any data source, regardless of the database vendor. The source code of the application doesn’t change whether it talks to Oracle or SQL Server. We only mention these two as an example. There are ODBC drivers available for several dozen popular database systems. Even Excel spreadsheets and plain text files can be turned into data sources. The operating system uses the Registry information written by ODBC Administrator to determine which low-level ODBC drivers are needed to talk to the data source (such as the interface to Oracle or SQL Server). The loading of the ODBC drivers is transparent to the ODBC application program. In a client/server environment, the ODBC API even handles many of the network issues for the application programmer.

The advantages of this scheme are so numerous that you are probably thinking there must be some catch. The only disadvantage of ODBC is that it isn’t as efficient as talking directly to the native database interface. ODBC has had many detractors make the charge that it is too slow. Microsoft has always claimed that the critical factor in performance is the quality of the driver software that is used. In our humble opinion, this is true. The availability of good ODBC drivers has improved a great deal recently. And anyway, the criticism about performance is somewhat analogous to those who said that compilers would never match the speed of pure assembly language. Maybe not, but the compiler (or ODBC) gives you the opportunity to write cleaner programs, which means you finish sooner. Meanwhile, computers get faster every year.

**JDBC**

In an effort to set an independent database standard API for Java; Sun Microsystems developed Java Database Connectivity, or JDBC. JDBC offers a generic SQL database access mechanism that provides a consistent interface to a variety of RDBMSs. This consistent interface is achieved through the use of “plug-in” database connectivity modules, or *drivers*. If a database vendor wishes to have JDBC support, he or she must provide the driver for each platform that the database and Java run on.

To gain a wider acceptance of JDBC, Sun based JDBC’s framework on ODBC. As you discovered earlier in this chapter, ODBC has widespread support on a variety of platforms. Basing JDBC on ODBC will allow vendors to bring JDBC drivers to market much faster than developing a completely new connectivity solution.

JDBC was announced in March of 1996. It was released for a 90-day public review that ended on June 8, 1996. Because of user input, the final JDBC v1.0 specification was released soon after.

The remainder of this section will cover enough information about JDBC for you to know what it is about and how to use it effectively. This is by no means a complete overview of JDBC. That would fill an entire book.

**JDBC Goals**

Few software packages are designed without goals in mind. JDBC is one that, because of its many goals, drove the development of the API. These goals, in conjunction with early reviewer feedback, have finalized the JDBC class library into a solid framework for building database applications in Java.

The goals that were set for JDBC are important. They will give you some insight as to why certain classes and functionalities behave the way they do. The eight design goals for JDBC are as follows:

1. **SQL Level API**

The designers felt that their main goal was to define a SQL interface for Java. Although not the lowest database interface level possible, it is at a low enough level for higher-level tools and APIs to be created. Conversely, it is at a high enough level for application programmers to use it confidently. Attaining this goal allows for future tool vendors to “generate” JDBC code and to hide many of JDBC’s complexities from the end user.

1. **SQL Conformance**

SQL syntax varies as you move from database vendor to database vendor. In an effort to support a wide variety of vendors, JDBC will allow any query statement to be passed through it to the underlying database driver. This allows the connectivity module to handle non-standard functionality in a manner that is suitable for its users.

1. **JDBC must be implemented on top of common database interfaces**  
    The JDBC SQL API must “sit” on top of other common SQL-level APIs. This goal allows JDBC to use existing ODBC-level drivers through the use of a software interface. This interface would translate JDBC calls to ODBC and vice versa.
2. **Provide a Java interface that is consistent with the rest of the Java system**

Because of Java’s acceptance in the user community thus far, the designers feel that they should not stray from the current design of the core Java system.

1. **Keep it simple**

This goal probably appears in all software design goal listings. JDBC is no exception. Sun felt that the design of JDBC should be very simple, allowing for only one method of completing a task per mechanism. Allowing duplicate functionality only serves to confuse the users of the API.

1. **Use strong, static typing wherever possible**

Strong typing allows for more error checking to be done at compile time; it also, appears at runtime.

1. **Keep the common cases simple**

Because more often than not, the usual SQL calls used by the programmer are simple SELECTs, INSERTs, DELETE and UPDATE, these queries should be simple to perform with JDBC. However, more complex SQL statements should also be possible. Finally, we decided to proceed with the implementation using Java Networking. And for dynamically updating the cache table we go for the MS Access database.

Java has two things: a programming language and a platform.

Java is a high-level programming language that is all of the following

Simple Architecture-neutral

Object-oriented Portable

Distributed High-performance

Interpreted multithreaded

Robust Dynamic

Secure

Java is also unusual in that each Java program is both compiled and interpreted. With a compile you translate a Java program into an intermediate language called Java byte codes the platform-independent code instruction is passed and run on the computer. Compilation happens just once; interpretation occurs each time the program is executed. The figure illustrates how this works.

**JavaProgram**

**Compilers**

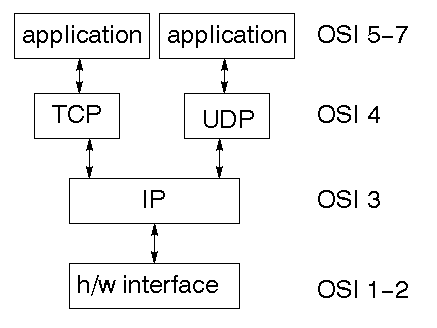
**Interpreter**

**My Program**

You can think of Java byte codes as the machine code instructions for the Java Virtual Machine (Java VM). Every Java interpreter, whether it’s a Java development tool or a Web browser that can run Java applets, is an implementation of the Java VM. The Java VM can also be implemented in hardware. Java byte codes help make “write once, run anywhere” possible. You can compile your Java program into byte codes on my platform which has a Java compiler. The byte codes can then be run in any implementation of the Java VM. For example, the same Java program can run Windows NT, Solaris, and Macintosh.

**Networking**

**TCP/IP stack :**The TCP/IP stack is shorter than the OSI one:



TCP is a connection-oriented protocol; UDP (User Datagram Protocol) is a connectionless protocol.

**IP datagram’s**

The IP layer provides a connectionless and unreliable delivery system. It considers each datagram independently of the others. Any association between datagram’s must be supplied by the higher layers. The IP layer supplies a checksum that includes its own header. The header includes the source and destination addresses. The IP layer handles routing through the Internet. It is also responsible for breaking up large datagram’s into smaller ones for transmission and reassembling them at the other end.

**UDP**

UDP is also connectionless and unreliable. What it adds to IP is a checksum for the contents of the datagram and port numbers. These are used to give a client/server model - see later.

**TCP**

TCP supplies logic to give a reliable connection-oriented protocol above IP. It provides a virtual circuit that two processes can use to communicate.

**Internet addresses**

In order to use a service, you must be able to find it. The Internet uses an address scheme for machines so that they can be located. The address is a 32-bit integer which gives the IP address. This encodes a network ID and more addressing. The network ID falls into various classes according to the size of the network address.

**Network address**

Class A uses 8 bits for the network address with 24 bits left over for other addressing. Class B uses a 16-bit network address. Class C uses 24-bit network addressing and class D uses all 32.

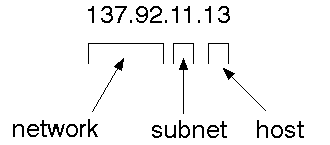
**Subnet address**

Internally, the UNIX network is divided into sub-networks. Building 11 is currently on one sub network and uses 10-bit addressing, allowing 1024 different hosts.

**Host address**

8 bits are finally used for host addresses within our subnet. This places a limit of 256 machines that can be on the subnet.

**Total address**



The 32-bit address is usually written as 4 integers separated by dots.

**Port addresses**

A service exists on a host and is identified by its port. This is a 16-bit number. To send a message to a server, you send it to the port for that service of the host that it is running on. This is not location transparency! Certain of these ports are "well known".

**Sockets**

A socket is a data structure maintained by the system to handle network connections. A socket is created using the calling socket. It returns an integer that is like a file descriptor. In fact, under Windows, this handle can be used with Read File and Write File functions.

#include <sys/types>

#include <sys/socket>

Int socket (int family, int type, int protocol);

Here "family" will be AF\_INET for IP communications, the protocol will be zero, and the type will depend on whether TCP or UDP is used. Two processes wishing to communicate over a network create a socket each. These are similar to two ends of a pipe - but the actual pipe does not yet exist.

**6.3 JFree Chart**

is a free 100% Java chart library that makes it easy for developers to display professional quality charts in their applications. Extensive feature set includes:

A consistent and well-documented API, supporting a wide range of chart types;

A flexible design that is easy to extend, and targets both server-side and client-side applications;

Support for many output types, including Swing components, image files (including PNG and JPEG), and vector graphics file formats (including PDF, EPS, and SVG);

JFree Chart is "open source" or, more specifically, [free software](http://www.gnu.org/philosophy/free-sw.html). It is distributed under the terms of the [GNU Lesser General Public License](http://www.gnu.org/licenses/lgpl.html) (LGPL), which permits use in proprietary applications.

***1.* Map Visualizations**

Charts showing values that relate to geographical areas. Some examples include (a) population density in each state of the United States, (b) income per capita for each country in Europe, and (c) life expectancy in each country of the world. The tasks in this project include:

Sourcing freely redistributable vector outlines for the countries of the world, states/provinces in particular countries (USA in particular, but also other areas);

Creating an appropriate dataset interface (plus default implementation), a rendered, and integrating this with the existing XY Plot class in JFree Chart;

Testing, documenting, testing some more, documenting some more.

***2.* Time Series Chart Interactivity**

Implement a new (to JFree Chart) feature for interactive time series charts --- to display a separate control that shows a small version of ALL the time series data, with a sliding "view" rectangle that allows you to select the subset of the time series data to display in the main chart.

**3. Dashboards**

There is currently a lot of interest in dashboard displays. Create a flexible dashboard mechanism that supports a subset of JFree Chart types (dials, pies, thermometers, bars, and lines/time series) that can be delivered easily via both Java Web Start and an applet.

**4. Property Editors**

The property editor mechanism in JFree Chart only handles a small subset of the properties that can be set for charts. Extend (or reemployment) this mechanism to provide greater end-user control over the appearance of the charts.

**J2ME (Java 2 Micro edition):-**

Sun Microsystems defines J2ME as "a highly optimized Java run-time environment targeting a wide range of consumer products, including pagers, cellular phones, screen-phones, digital set-top boxes, and car navigation systems." Announced in June 1999 at the JavaOne Developer Conference, J2ME brings the cross-platform functionality of the Java language to smaller devices, allowing mobile wireless devices to share applications. With J2ME, Sun has adapted the Java platform for consumer products that incorporate or are based on small computing devices.

**1. General J2ME architecture**



J2ME uses configurations and profiles to customize the Java Runtime Environment (JRE). As a complete JRE, J2ME is comprised of a configuration, which determines the JVM used, and a profile, which defines the application by adding domain-specific classes. The configuration defines the basic run-time environment as a set of core classes and a specific JVM that run on specific types of devices. We'll discuss configurations in detail in the profile that defines the application; specifically, it adds domain-specific classes to the J2ME configuration to define certain uses for devices. We'll cover profiles in depth in the following graphic depicts the relationship between the different virtual machines, configurations, and profiles. It also draws a parallel with the J2SE API and its Java virtual machine. While the J2SE virtual machine is generally referred to as a JVM, the J2ME virtual machines, KVM and CVM, are subsets of JVM. Both KVM and CVM can be thought of as a kind of Java virtual machine -- it's just that they are shrunken versions of the J2SE JVM and are specific to J2ME.

1. **Developing J2ME applications**

Introduction In this section, we will go over some considerations you need to keep in mind when developing applications for smaller devices. We'll take a look at the way the compiler is invoked when using J2SE to compile J2ME applications. Finally, we'll explore packaging and deployment and the role pre-verification plays in this process.

1. **Design considerations for small devices**

Developing applications for small devices requires you to keep certain strategies in mind during the design phase. It is best to strategically design an application for a small device before you begin coding. Correcting the code because you failed to consider all of the "gotchas" before developing the application can be a painful process. Here are some design strategies to consider:

\* Keep it simple. Remove unnecessary features, possibly making those features a separate, secondary application.

\* Smaller is better. This consideration should be a "no-brainer" for all developers. Smaller applications use less memory on the device and require shorter installation times. Consider packaging your Java applications as compressed Java Archive (jar) files.

\* Minimize run-time memory use. To minimize the amount of memory used at run time, use scalar types in place of object types. Also, do not depend on the garbage collector. You should manage the memory efficiently yourself by setting object references to null when you are finished with them. Another way to reduce run-time memory is to use lazy instantiation, only allocating objects on an as-needed basis. Other ways of reducing overall and peak memory use on small devices are to release resources quickly, reuse objects, and avoid exceptions.

**4. Configurations overview**

The configuration defines the basic run-time environment as a set of core classes and a specific JVM that run on specific types of devices. Currently, two configurations exist for J2ME, though others may be defined in the future:

\* **Connected Limited Device Configuration (CLDC)**is used specifically with the KVM for 16-bit or 32-bit devices with limited amounts of memory. This is the configuration (and the virtual machine) used for developing small J2ME applications. Its size limitations make CLDC more interesting and challenging (from a development point of view) than CDC. CLDC is also the configuration that we will use for developing our drawing tool application. An example of a small wireless device running small applications is a Palm hand-held computer.

\* **Connected Device Configuration (CDC)**is used with the C virtual machine (CVM) and is used for 32-bit architectures requiring more than 2 MB of memory. An example of such a device is a Net TV box.

**5. J2ME profiles**

**What is a J2ME profile?**

As we mentioned earlier in this tutorial, a profile defines the type of device supported. The Mobile Information Device Profile (MIDP), for example, defines classes for cellular phones. It adds domain-specific classes to the J2ME configuration to define uses for similar devices. Two profiles have been defined for J2ME and are built upon CLDC: KJava and MIDP. Both KJava and MIDP are associated with CLDC and smaller devices. Profiles are built on top of configurations. Because profiles are specific to the size of the device (amount of memory) on which an application runs, certain profiles are associated with certain configurations. A skeleton profile upon which you can create your own profile, the Foundation Profile, is available for CDC.

**Profile 1: KJava**

KJava is Sun's proprietary profile and contains the KJava API. The KJava profile is built on top of the CLDC configuration. The KJava virtual machine, KVM, accepts the same byte codes and class file format as the classic J2SE virtual machine. KJava contains a Sun-specific API that runs on the Palm OS. The KJava API has a great deal in common with the J2SE Abstract Windowing Toolkit (AWT). However, because it is not a standard J2ME package, its main package is com.sun. Java We'll learn more about the KJava API later in this tutorial when we develop some sample applications.

**Profile 2: MIDP**

MIDP is geared toward mobile devices such as cellular phones and pagers. The MIDP, like KJava, is built upon CLDC and provides a standard run-time environment that allows new applications and services to be deployed dynamically on end-user devices. MIDP is a common, industry-standard profile for mobile devices that is not dependent on a specific vendor. It is a complete and supported foundation for mobile application

development. MIDP contains the following packages, the first three of which are core CLDC packages, plus three MIDP-specific packages.

\* java.lang

\* java.io

\* java.util

\* javax.microedition.io

\* javax.microedition.lcdui

\* javax.microedition.midlet

\* javax.microedition.rms

**SYSTEM DESIGN**

**UML DIAGRAMS**

UML stands for Unified Modeling Language. UML is a standardized general-purpose modeling language in the field of object-oriented software engineering. The standard is managed, and was created by, the Object Management Group. The goal is for it to become a common language for creating models of object oriented computer software. In its current form UML is comprised of two major components: aMeta-model and a notation. In the future, some form of method or process may also be added to; or associated with, UML.

The Unified Modeling Language is a standard language for specifying, Visualization, Constructing and documenting the artifacts of software system, as well as for business modeling and other non-software systems.

The UML represents a collection of best engineering practices that have proven successful in the modeling of large and complex systems.

The UML is a very important part of developing objects oriented software and the software development process. The UML uses mostly graphical notations to express the design of software projects.

GOALS:

1. Provide users a ready-to-use, expressive visual modeling Language so that they can develop and exchange meaningful models.

2. Provide extendibility and specialization mechanisms to extend the core concepts.

3. Be independent of particular programming languages and development process.

4. Provide a formal basis for understanding the modeling language.

5. Encourage the growth of OO tools market.

6. Support higher level development concepts such as collaborations, frameworks, patterns and components.

7. Integrate best practices.

###### USE CASE DIAGRAM:

In the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Role of the actors in the system can be depicted.

**CLASS DIAGRAM:**

In software engineering, a class diagram in the Unified Modeling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among the classes. It explains which class contains information.

**SEQUENCE DIAGRAM:**

A sequence diagram in Unified Modeling Language (UML) is a kind of interaction diagram that shows how processes operate with one another and in what order. It is a construct of a Message Sequence Chart. Sequence diagrams are sometimes called event diagrams, event scenarios, and timing diagrams.

**ACTIVITY DIAGRAM:**

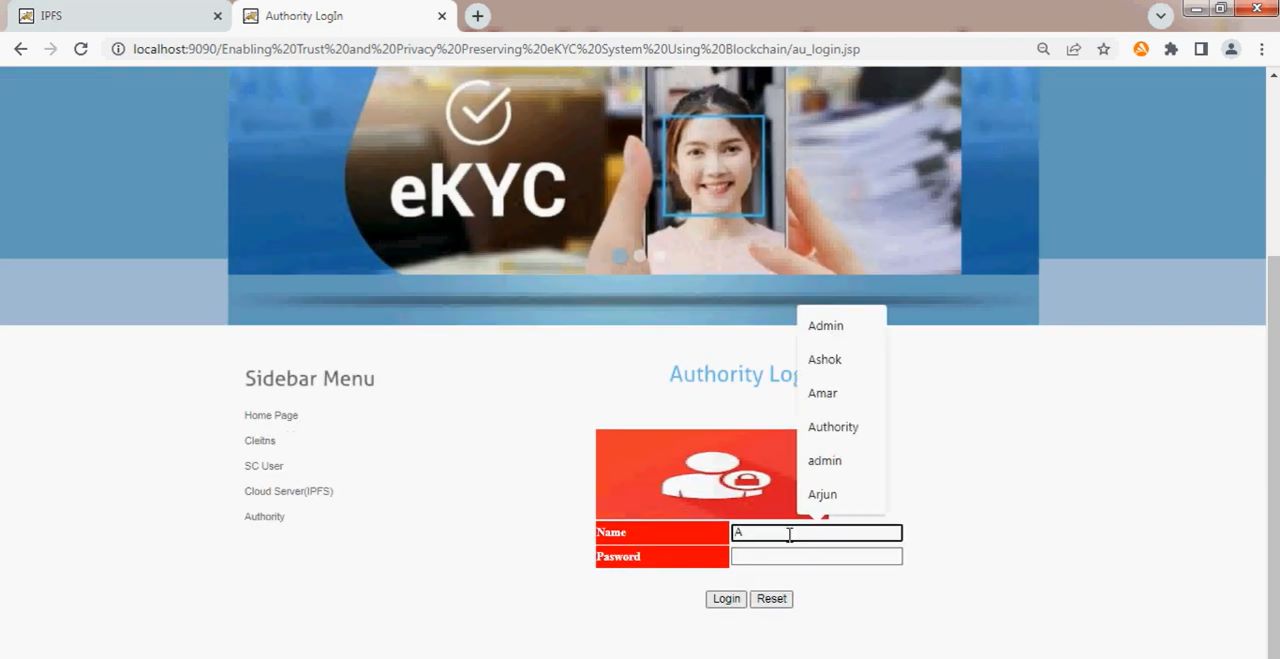
Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modeling Language, activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system. An activity diagram shows the overall flow of control.

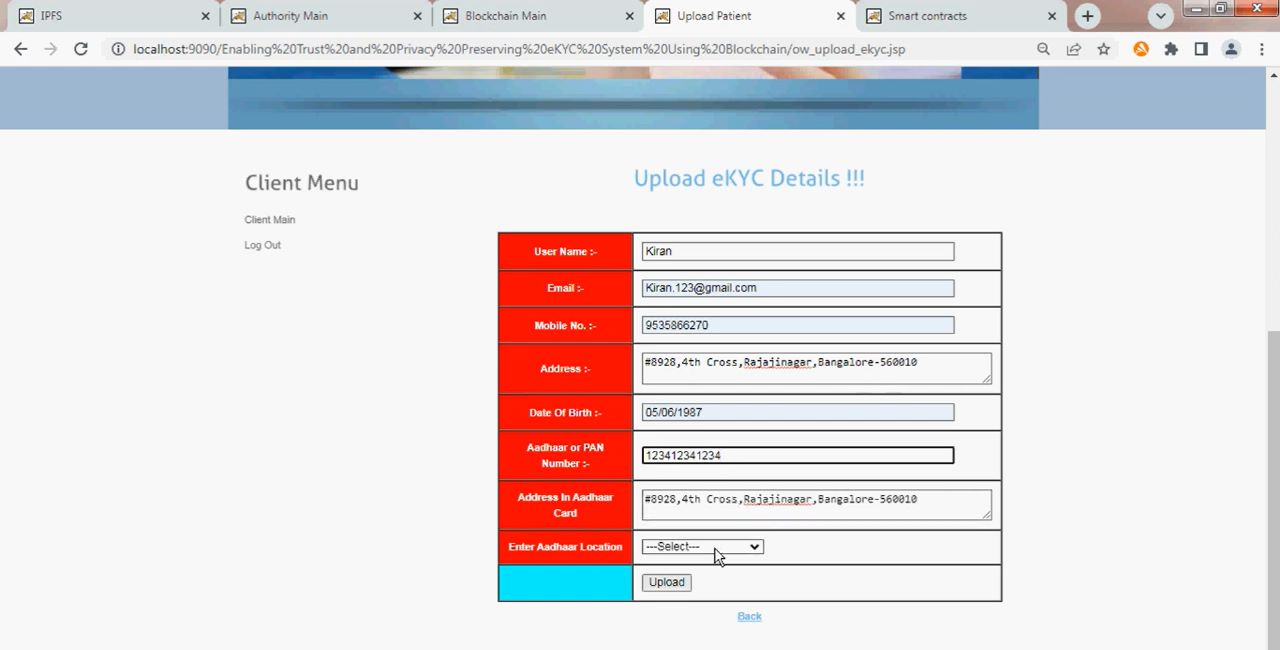
**SYSTEM TESTING**

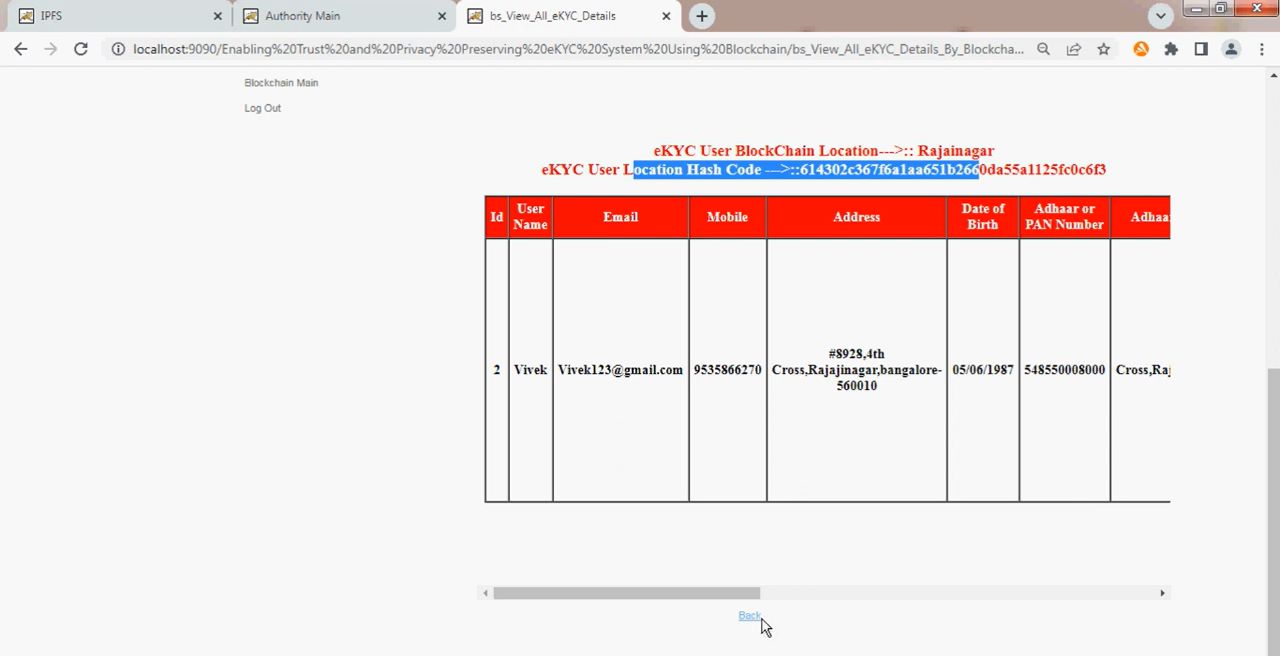
Software once validated must be combined with other system elements (e.g. Hardware, people, database). System testing verifies that all the elements are proper and that overall system function performance is

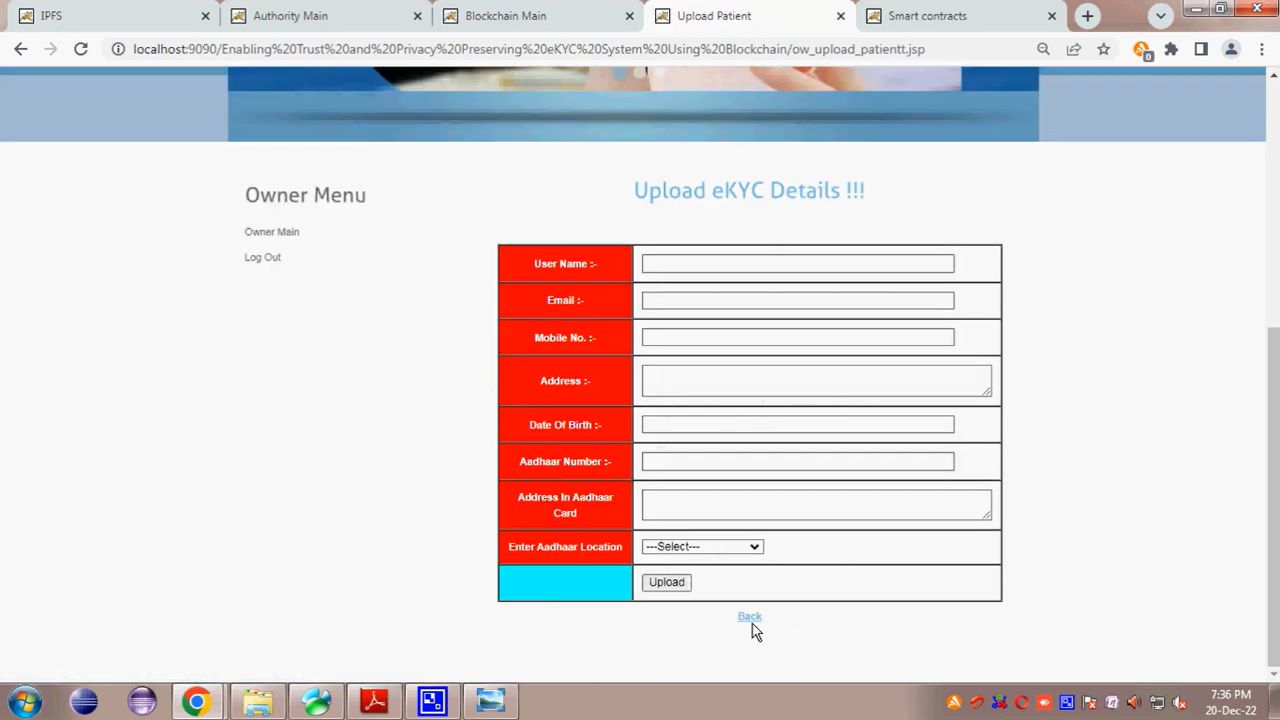
achieved. It also tests to find discrepancies between the system and its original objective, current specifications, and system documentation.

**RESULT:**

****

****

****

****

**CONCLUSION:**

We have presented the privacy-preserving e-KYC approach based on the blockchain. Our proposed scheme delivers secure and decentralized authentication and verification of the e-KYC process with the user’s consent enforcement feature. In our scheme, the privacy of both customers’ identity documents stored in the cloud is guaranteed by the symmetric key and public key encryption while the sensitive transaction data stored in the blockchain is encrypted by symmetric key encryption and CP-ABE. Our scheme also allows the KYC data to be updated by the data owner or the customer. In addition, we devised an access policy update algorithm to enable dynamic access authorization. For the evaluation, we performed comparative analysis between our scheme and related works in terms of the computation cost, the communication cost, and performance. The experimental results showed that our scheme outperforms existing schemes in terms of performance, comprehensive KYC compliance features, and the scalable access control mechanism. For future works, we will test a larger sample of data in the real cloud environment and measure the throughput of the system in accommodating high number of e-KYC registration and verification requests. In addition, we will investigate the technique to enable batch verification of e-KYC transactions stored in the block chain with the searchable encryption feature.

**REFERENCES:**

[1] Y. Zhong, M. Zhou, J. Li, J. Chen, Y. Liu, Y. Zhao, and M. Hu, ‘‘Distributed blockchain-based authentication and authorization protocol for smart grid,’’ Wireless Commun. Mobile Comput., vol. 2021, pp. 1–15, Apr. 2021, doi: 10.1155/2021/5560621.

[2] S. Y. Lim, P. T. Fotsing, A. Almasri, O. Musa, M. L. M. Kiah, T. F. Ang, and R. Ismail, ‘‘Blockchain technology the identity management and authentication service disruptor: A survey,’’ Int. J. Adv. Sci. Eng. Inf. Tech., vol. 8, pp. 1735–1745, Sep. 2018.

[3] A. A. Mamun, A. Al Mamun, S. R. Hasan, S. R. Hasan, M. S. Bhuiyan, M. S. Bhuiyan, M. S. Kaiser, M. S. Kaiser, M. A. Yousuf, and M. A. Yousuf, ‘‘Secure and transparent KYC for banking system using IPFS and blockchain technology,’’ in Proc. IEEE Region Symp. (TENSYMP), Jun. 2020, pp. 348–351.

[4] M. Pic, G. Mahfoudi, and A. Trabelsi, ‘‘Remote KYC: Attacks and countermeasures,’’ in Proc. Eur. Intell. Secur. Informat. Conf. (EISIC), Nov. 2019, pp. 126–129.

[5] W. Shbair, M. Steichen, and J. François, ‘‘Blockchain orchestration and experimentation framework: A case study of KYC,’’ in Proc. 1st IEEE/IFIP Int. Workshop Manag. Managed Blockchain (Man Block), Jeju Island, South Korea, Aug. 2018, pp. 23–25.

[6] 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, doi: 10.1109/BLOC.2019.8751480.

[7] T. Mikula and R. H. Jacobsen, ‘‘Identity and access management with blockchain in electronic healthcare records,’’ in Proc. 21st Euromicro Conf. Digit. Syst. Design (DSD), Prague, Czech Republic, Aug. 2018, pp. 699–706.

[8] S. Wang, R. Pei, and Y. Zhang, ‘‘EIDM: A ethereum-based cloud user identity management protocol,’’ IEEE Access, vol. 7, pp. 115281–115291, 2019, doi: 10.1109/ACCESS.2019.2933989.

[9] N. Ullah, K. A. Al-Dhlan, and W. M. Al-Rahmi, ‘‘KYC optimization by blockchain based hyperledger fabric network,’’ in Proc. 4th Int. Conf. Adv. Electron. Mater., Comput. Softw. Eng. (AEMCSE), Mar. 2021, pp. 1294–1299.

[10] 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. 41, pp. 1–13, 2020.

[11] J. Bethencourt, A. Sahai, and B. Waters, ‘‘Ciphertext-policy attribute-based encryption,’’ in Proc. IEEE Symp. Secur. Privacy, Oakland, CA, USA, May 2007, pp. 321–334.

[12] I. Gutierrez-Aguero, S. Anguita, X. Larrucea, A. Gomez-Goiri, and B. Urquizu, ‘‘Burnable pseudo-identity: A non-binding anonymous identity method for ethereum,’’ IEEE Access, vol. 9, pp. 108912–108923, 2021.

[13] S. Nakamoto. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Accessed: Jan. 8, 2022. [Online]. Available: <https://bitcoin.org/bitcoin.pdf>

[14] J. P. Moyano and O. Ross, ‘‘KYC optimization using distributed ledger technology,’’ Bus. Inf. Syst. Eng., vol. 59, no. 6, pp. 411–423, Dec. 2017.

[15] A. Chowdhary, S. Agrawal, and B. Rudra, ‘‘Blockchain based framework for Student identity and educational certificate verification,’’ in Proc. 2nd Int. Conf. Electron. Sustain. Commun. Syst. (ICESC), Aug. 2021, pp. 916–921.

[16] GDPREuropeanUnionGuidelines. Accessed: Aug. 12, 2021. [Online]. Available: <https://gdprinfo.eu/>

[17] G. Bramm, M. Gall, and J. Schütte, ‘‘BDABE-blockchain-based distributed attribute based encryption,’’ in Proc. 15th Int. Conf. e-Bus. Telecommun., 2018, pp. 99–110.

[18] Y. Fan, X. Lin, W. Liang, J. Wang, G. Tan, X. Lei, and L. Jing, ‘‘TraceChain: A blockchain-based scheme to protect data confidentiality and traceability,’’ Softw., Pract. Exper., vol. 52, no. 1, pp. 115–129, Jan. 2022, doi: 10.1002/spe.2753.

[19] C. Yuan, M. Xu, X. Si, and B. Li, ‘‘Blockchain with accountable CP-ABE: How to effectively protect the electronic documents,’’ in Proc. IEEE 23rd Int. Conf. Parallel Distrib. Syst. (ICPADS), Dec. 2017, pp. 800–803.

[20] A. Wu, Y. Zhang, X. Zheng, R. Guo, Q. Zhao, and D. Zheng, ‘‘Efficient and privacy-preserving traceable attribute-based encryption in blockchain,’’ Ann. Telecommun., vol. 74, nos. 7–8, pp. 401–411, Aug. 2019.

[21] L. Guo, X. Yang, and W.-C. Yau, ‘‘TABE-DAC: Efficient traceable attribute-based encryption scheme with dynamic access control based on blockchain,’’ IEEE Access, vol. 9, pp. 8479–8490, 2021, doi: 10.1109/ACCESS.2021.3049549.

[22] M. Barati, G. S. Aujla, J. T. Llanos, K. A. Duodu, O. F. Rana, M. Carr, and R. Ranjan, ‘‘Privacy-aware cloud auditing for GDPR compliance verification in online healthcare,’’ IEEE Trans. Ind. Informat., vol. 18, no. 7, pp. 4808–4819, Jul. 2022, doi: 10.1109/TII.2021.3100152.

[23] PBC (Pairing-Based Cryptography) Library. Accessed: Jan. 5, 2022. [Online]. Available: <https://crypto.stanford.edu/pbc/>

[24] S. Gao, G. Piao, J. Zhu, X. Ma, and J. Ma, ‘‘TrustAccess: A trustworthy secure ciphertext-policy and attribute hiding access control scheme based on blockchain,’’ IEEE Trans. Veh. Technol., vol. 69, no. 6, pp. 5784–5798, Jun. 2020.

[25] A. D. Dwivedi, R. Singh, U. Ghosh, R. R. Mukkamala, A. Tolba, and O. Said, ‘‘Privacy preserving authentication system based on noninteractive zero knowledge proof suitable for Internet of Things,’’ J. Ambient Intell. Humanized Comput., pp. 1–11, Sep. 2021, doi: 10.1007/s12652- 021-03459-4.

[26] K. Bhaskaran, P. Ilfrich, D. Liffman, C. Vecchiola, P. Jayachandran, A. Kumar, F. Lim, K. Nandakumar, Z. Qin, V. Ramakrishna, E. G. Teo, and C. H. Suen, ‘‘Double-blind consent-driven data sharing on blockchain,’’ in Proc. IEEE Int. Conf. Cloud Eng. (IC E), Apr. 2018, pp. 385–391.

[27] F. Ghaffari, E. Bertin, N. Crespi, S. Behrad, and J. Hatin, ‘‘A novel access control method via smart contracts for internet-based service provisioning,’’ IEEE Access, vol. 9, pp. 81253–81273, 2021.

[28] (Jan. 2016). Know Your Customer: Quick Reference Guide, Understanding Global KYC differences by PWC. Accessed: Feb. 28, 2022. [Online]. Available: https://www.pwc.com/gx/en/financial-services/publications/ assets/pwc-anti-money-laundering-know-your-customer-quick-referenceguide.pdf

[29] (2018). Technical Standard for Digital Identification Systems Published by World Bank Group. Accessed: Feb. 28, 2022. [Online]. Available: https://olc.worldbank.org/system/files/129743-WP-PUBLIC-ID4DCatalog-of-Technical-Standards.pdf

[30] European Commission’s Expert Sub Working Group 1, Electronic Identification and Remote Know Your Customer Processes. Accessed: Feb. 28, 2022. [Online]. Available: https://ec.europa.eu/info/ sites/default/files/business\_economy\_euro/banking\_and\_ finance/documents/report-on-existing-remote-on-boarding-solutionsin-the-banking-sector-december2019\_en.pdf

[31] C. Dannen, Introducing Ethereum and Solidity. Berkeley, CA, USA: Apress, 2017. [Online]. Available: https://link.springer. com/book/10.1007/978-1-4842-2535-6