ISSN: 0974-8571 Vol.13 No. 2 December, 2021

International Journal of Computational Intelligence in Control

A Model for Secure Inter-Institutional Communication Based on Artificial Intelligence (AI) and Blockchain

Mir Rahib Hussain Talpur[1], Mir Sajjad Hussain Talpur[1], Fauzia Talpur[2], Abdul Haseeb[1], Asadullah Kehar[3], Shereen Fatima[4]

[1]Information Technology Centre, Sindh Agriculture University Tandojam, Sindh, Pakistan
[2]University of Sindh Laar Campus@Badin
[3]Department of Computer Science, Shah Abdul Latif University, Khairpur
[4]Department of Computer Science, Shaikh Ayaz University, Shikarpur
*Corresponding Author: mirsajjadhussain@sau.edu.pk

ABSTRACT: **Communication between different organisations and within different components of the organization itself is one of the trending issues nowadays. Over the past year, it has proven to be essential for many businesses left short on staff due to COVID-19, and communications have shifted from face-to-face to calls and emails. In the corporate world, communication is essential, and information technology provides our firm with the tools it needs to communicate quickly and effectively. Information technology can benefit our company by allowing for faster communication, electronic storage, and record protection. Organizations, whether they are educational institutes or any commercial organization, contain sensitive data which is meant to be kept confidential and integrated, depending upon the nature of the data. Different organisations may include several components, i.e., educational institutions such as universities consist of several faculties or departments and administrative departments, while commercial organisations consist of many departments. The administrative department can be far away from the other departments, though the letter issued can be changed by any harmful person, and data that is incorporated into the letter can be exploited and attacked. Keeping these problems in mind, this research was planned to overcome the above issues of security by using trending technologies, including blockchain, by designing a secure model that can be used to solve the confidentiality issues and integrity issues of communication between different organisations and inter-organizational communication to exchange information and data between and in-between them. In the proposed model, departments and distributed servers will be connected with each other with the help of an interface. In the departments, the administrators of personals will be authenticated and authorized by credentials and biometrics to keep the data secure. To communicate, a read/write request will be sent to the server, and the output of that request will be shown on the department side. To keep the data secure and untemper able, it was stored in a blockchain structure. Each block contained the data and was connected with other blocks. The proposed model was also validated by calculating empirical results in which a sample application was developed and tested three times at Sindh Agriculture University Tandojam while varying the different scenarios. The results proved the proposed model to be secure and easy to use. However, it also increased the confidentiality and integrity of the data.**

Keywords: Blockchain, AI, Secure communication

1. INTRODUCTION

The benefits of information technology are directed towards the world of business and organizations, allowing them to perform work in an efficient way and to maximize productivity [1]. People in the industry are searching for new ways to get more work done quickly, so this should only be possible as information technology advances. Our organization can profit from information technology by offering instant communication, information storage, and data protection [2]. Information technology systems are a collection of advanced technological devices that assist in the delivery of essential data to managers who want to use that data to make critical choices regarding their company's operations. Computer programmes, which are employed in practically every business scenario, are referred to as information technology [3]. It is beneficial to include information technology in our firm because computerized systems are so widely used. Digital storage systems are created by information technology to protect our

industry's valuable records [4]. Customer and customer file security is vital to any organization's success. Information Technology (IT) is a set of tools, processes, and procedures including programming or coding, data transfer, data processing, retrieval of information, systems analysis and design, and control systems, as well as supporting equipment for collecting, analyzing, and presenting data [5].

Students' ability to keep their employment and go to university is largely dependent on information technology. The corporate world was transformed with the arrival of computers, and organisations now use information technology to guarantee that their departments work efficiently [6]. We could work at home or even on the road thanks to IT technologies that provide us with remote access to our company's online platform. Because we can still get work completed even if we're not in the office, this availability allows us to boost our performance [7]. In the corporate world, communication is essential, and information technology provides our firm with the tools it needs to communicate quickly and effectively [8]. Our information technology team can set up the internet. We provide virtual meeting devices and confidential chat sessions for our employees so that they can handle business and always interact effectively [9]. Different organisations may include several components, i.e., educational institutions such as universities consist of a number of faculties or departments and administrative departments, while commercial organisations consist of many departments. Each department/faculty includes a number of stakeholders, such as workers, managers, customers, etc. However, communication between different organisations and within different components of the organisation itself is one of the trending issues nowadays. Organizations, whether they are educational institutes or any commercial organization, contain sensitive data which is meant to be kept confidential and integrated, depending upon the nature of the data. In the case of universities, administrative departments issue confidential letters to different heads of departments or teachers. Those letters must be kept confidential so that no unauthorised person can read them. The administrative department can be far away from the other departments, though the letter issued can be changed by any harmful person, and data that is incorporated into the letter can be exploited and attacked. Keeping the above problems in mind, this research is planned to overcome the above issues of security by using trending technologies, including blockchain. This research is planned to design a secure model that can be used to solve the confidentiality issues and integrity issues of communication between different organisations and inter-organizational communication to exchange information and data between and in-between them.

The AI and blockchain-based secure institutional communication model will provide a secure platform to share official and confidential information between different entities within the department or organization. This model will also cause an increase in the integrity of the user's data so that no third party can change the official information once it is deployed or shared. This behavior of the model will ultimately increase the confidentiality and integrity of data between different organizations, departments, and entities. This research will also be responsible for bringing Artificial Intelligence and Blockchain Technologies for secure communication. In this study, we designed a secure inter-institutional communication model by using AI and blockchain, incorporated confidentiality and integrity into the designed model, and validated the designed secure inter-institutional communication model.

2. LITERATURE REVIEW

2.1 AI and Blockchain Data Security

AI improves the security of blockchain-based security solutions by allowing users to manage their data more quickly and ensuring that the data and models generated from it are more dependable, fair, and trustworthy [10]. Through decentralised identification and other privacy features, blockchain and distributed ledger technologies offer innovative potential for securing customer data. These systems can provide consumers more control over their data by providing tools that allow them to own and govern it. Artificial intelligence expands the range of possibilities for systems and customer security, data enrichment, and superior analysis methods [11]. Blockchain and Artificial Intelligence technologies are rapidly growing, allowing for new ways to share and combine data that were previously unthinkable. Simultaneously, technological improvements open up new possibilities for the ethical use of data [12]. When personal data is shared, it poses a quandary for both businesses and individuals because it can provide major benefits while also providing significant risks and costs to both the individual and the organisations with which personal data is shared [13]. Blockchain enables new mechanisms for data transmission that respect individual privacy and give people control over their own data, such as decentralized identity and zero knowledge evidence [13].

In the last few years, in the scientific community, artificial intelligence and blockchain-based technologies have gained a strong reputation. Massive volumes of data can now be processed by AI, while blockchain provides for decentralized and secure data access [15]. Universities must digitize in order to enhance and improve their services and make them more accessible to beneficiaries [16]. Universities may become more productive, efficient, adaptable, and comfortable by implementing new technologies [17]. The concept of a smart university, which represents higher education in the digital age, has substantially intensified these considerations, and in our era, blockchain is one of the most rapidly expanding technologies [18].

2.2 AI Enhances Blockchain Security

The potential of blockchain technology to handle problems like double spend, consent, data integrity, transactional trust, identity, and overall information security appears to be driving its revolution and evolution [19]. The substance of what is recorded on the ledger, the procedure used to obtain consensus, and the degree to which the ledger is permissioned will all influence the design of such blockchain applications [20]. Because blockchain enables openness and accountability over which users' data is accessible, when, and under what, it can incentivize data sharing [21]. As blockchain gives control of data to users, people will have more faith in sharing data and understanding that their data will be used responsibly to enable better personalization or for other good causes [22]. Blockchain is not just the kind of internet support based on distributed statements, except with a different supply from the equipment connection system. In general, blockchain is a distributed

system of machines (blocks) that is managed to track the origin of knowledge distribution [23]. Every block keeps some safety and precision in the data by containing a full collection of records of earlier activities [24]. While a new node is acting as designed through a worker, that is the primary unit proving every activity in the node plus completing a numerical query and producing a digital stamp for the nodes, which join a pre-defined operation that applies the hash function [25]. The newly generated block directions are transmitted over all of the blockchain channels, enabling each block to similarly control the full record [26]. One of the most essential features for a blockchain is to perform high-efficiency traceability in some fields, such as food supply and educational services that involve superior smart context-aware services and applications for university learners and staff. High-efficient traceability has been used to allow blockchain members to obtain decisions and correlative outlines quickly and adaptably. High-efficient traceability combined with smart things can assist companies with reaching their educational achievements through further adaptability and at lower costs [27]. Data provenance can operate with smart devices as a variety of records and proof of experience for the following devices and methods of action, such as enhancing the instruction, education, and assessment processes included in smart universities and fostering analysis and discovery. The data provenance could be performed by preparing information; for example, all members' actions and environmental knowledge stream, obtained via smart sensors [28]. The application of smart devices and IoT for tracking data origins in the blockchain system means knowledge of the processes' secure strength, particularly in evaluating learners for instructional certificate security protection. IoT can be used in conjunction with existing adult data provenance security practices, such as implementing its hash/signature chain structure for integrity strength and entrance check procedures for confidentiality protection, as well as determining those safety issues that arise with smart things for performing other valuable administrative actions [29].

The absence of intrinsic security in system forecasts is now preventing AI-powered intelligent systems from being used in the actual world [30]. Blockchain is a well-known technology that can assist in addressing the security concerns that AI applications raise. Both of these technologies are complementary in that Blockchain can assist AI in overcoming its shortcomings, and AI can assist Blockchain in performing better [31]. Many studies on the use of Blockchains to secure intelligent applications in a variety of vital sectors, including medicine, finance, industry, administration, and defence, are now underway. However, there is a paucity of thorough research in this sector that may provide an overview of current research activities in using Blockchains to protect and improve the resilience of Artificial Intelligence-based systems [32]. Through statistical and literary analysis, this study investigates how Blockchain serves as a support system for AI-based systems. Blockchain technology is a new internet and digital world trend that offers high degrees of security. The available security measures are based on centralized servers/systems. In this arrangement, single points of failure, exposure to security issues, and the need for third-party suppliers are all negatives [2]. Blockchain technology, on the other hand, is a decentralized system in which no third parties can be trusted and confidence is built among the network's nodes. Bitcoin, Ether, and Ripple were the first cryptocurrencies to use blockchain technology [33] developed technology. After learning about the key capabilities of Blockchain technology, many researchers came up with the idea of applying it to various industrial applications such as voting, healthcare, finance, and supplier management to meet the integrity, accessibility, and confidentiality requirements without the involvement of a centralized authority [34].

3. RESEARCH METHODOLOGY

This research was divided into three phases. In the first phase, a secure inter-communicational model was designed, which was further validated by developing a desktop application and testing it in the Sindh Agriculture University Tandojam. In the last phase, security parameters were incorporated and tested in order to make the application more and more secure.

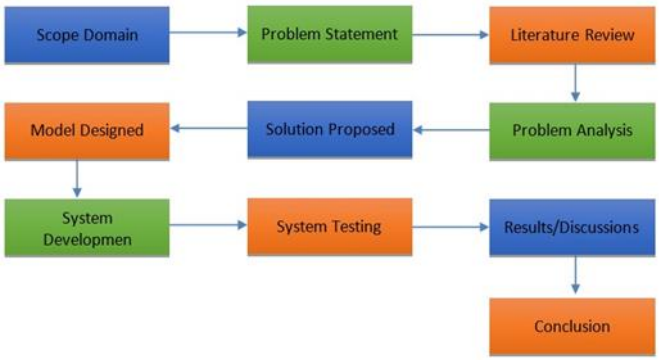

Figure 3.1: Overall Research Methodology

3.1 DESIGNING THE INTER-INSTITUTIONAL COMMUNICATION MODEL

Figure 3.2 represents the designed or proposed model for secure inter-institutional communication model.

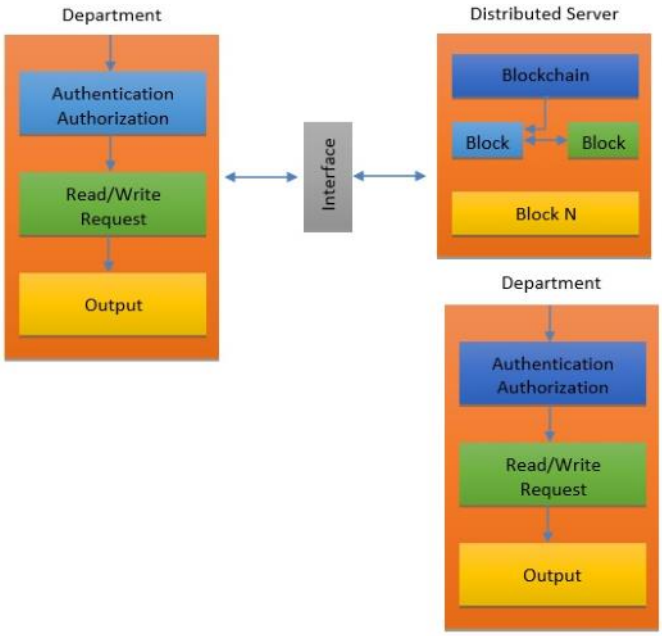

Figure 3.2: Proposed Model for Secure Inter-Institutional Communication

With the help of an interface, departments and distributed servers will relate to each other. In the departments, the administrators of personals will be authenticated and authorized by credentials and biometrics to keep the data secure. After authentication and authorization, to communicate, a read or write request will be sent to the server and the output of that request will be shown on the department side. To keep the data secure and un-temperable data will be stored in a blockchain on the distributed server. Each block will contain the data and will be connected to other blocks.

A blockchain is considered a special type of database in which data is stored in blocks. Each block is connected to its next and previous block, forming a chain. In contrast, blockchain is decentralized, though in the designed model, different decentralized and distributed servers will be used. In our case, different clouds will be used as those distributed servers. A common interface will also be designed to get access to those servers. This interface will be used as an intermediator between the department and those distributed servers. Since a university may consist of different faculties, each faculty may include several departments. Each department will use an interface to get access to distributed servers. To communicate between different departments, each department will have to send and receive requests. The request will contain the data and other necessary information. That request will be sent to distributed servers with the help of an interface designed. The flow of communication between departments, interfaces, and different distributed servers is depicted in figure 3.3.

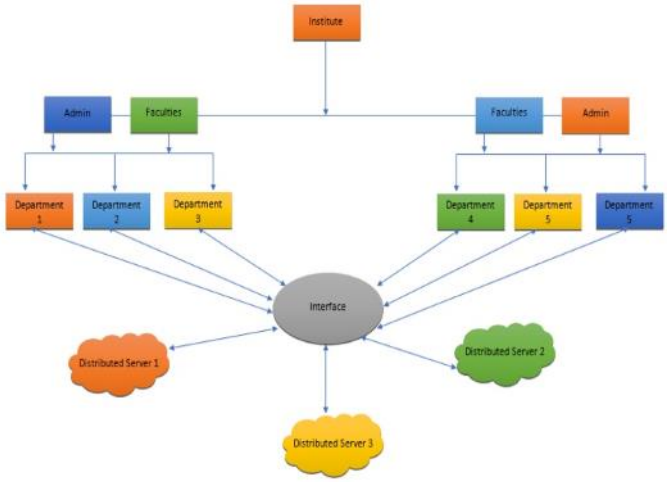

Figure 3.3: Flow of communication in the proposed model

3.2 ***VALIDATING THE DESIGNED FRAMEWORK***

To validate the designed framework, a smart application was developed using the Python programming language. This application was compatible with Microsoft Windows and could run on any version of Microsoft Windows. The designed application was further tested through different evaluations, i.e., 3 tests were conducted at Sindh Agriculture University Tandojam during the months of July and August 2021. For designing and developing applications, the following tools and techniques are used.

1) Hardware

The physical components that a computer system requires to function are known as computer hardware. It includes the motherboard, graphics card, CPU (Central Processing Unit), ventilation fans, webcam, power supply, and other circuit board components that operate within a PC or laptop. In our developed system, a desktop computer or laptop was used to validate and authorize the user to exchange information in the inter-institutional communication application.

2) Software

Hardware is frequently controlled by a platform, which is known as software. It contains a collection of data and instructions that are divided into two categories: Before the user can use the operating system (Windows XP), System Software needs to check all hardware such as the printer, mouse, keyboard, monitor, and hard drive DVD drive. The software that integrates the hardware and the user via graphical interfaces is known as operating system software. It has a set of non-task special tasks that assist the user in controlling, managing, and integrating individual hardware. Application software is a type of software that aids in the completion of specific tasks. It could contain a single programme or a collection of programmes. System software includes things like Windows, UNIX, LINUX, and OS X, while application software includes things like image viewers, text and spreadsheet editors, video and audio players, and so on. Application Software that allows a user to meet their needs, e.g., Building CVs are a term used to describe

the process of creating a curriculum vitae. Presentations (PowerPoint) Budgeting and forecasting in Excel Database access We are going to post free system solutions so researchers can try to discover our assignment writing services and get an overview of the quality of work. Components of a Computer System are given by the industry's topmost qualified writers with the assurance of excellent marks. In our developed system, the Microsoft Windows operating system was used.

3.3 APPLICATION TESTING

An empirical study was conducted at Sindh Agriculture University Tandojam, in which the developed application was tested through 3 different evaluations. In each of the evaluations, the application was opened and (Figure 3.4) a login screen was shown. When the unauthentic credentials were provided, the application did not proceed.

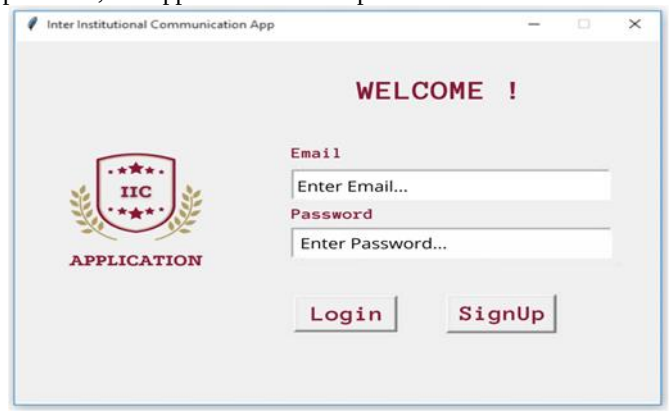

Figure 3.4: The login screen for an inter-institutional communication application that has been developed

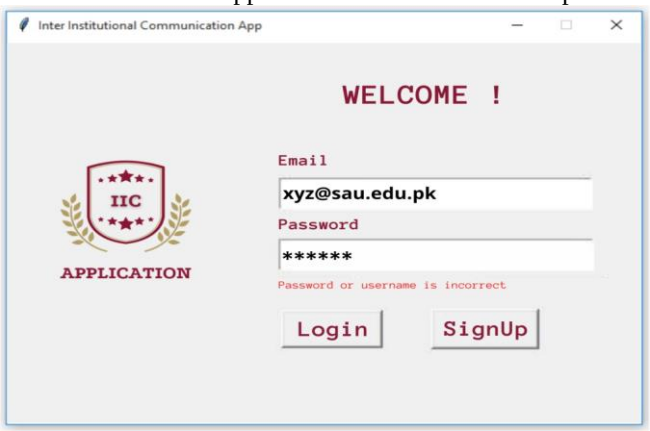

Figure 3.5: Login Screen of a developed inter-institutional communication application showing an error message

First, when the application window was opened, it asked for the registered email and password. When the username and password were matched with the registered person, biometric authentication came into place. Once the face detection window was opened for face detection and recognition, that person had to place his or her face in front of the camera so that the application could recognize his or her face for login. If in Figure 3.6, if the person is not officially authorized by the system, then the failure notification will occur. However, if the registered person's face has been recognized and detected, then it has successfully logged in and may proceed to the home page.

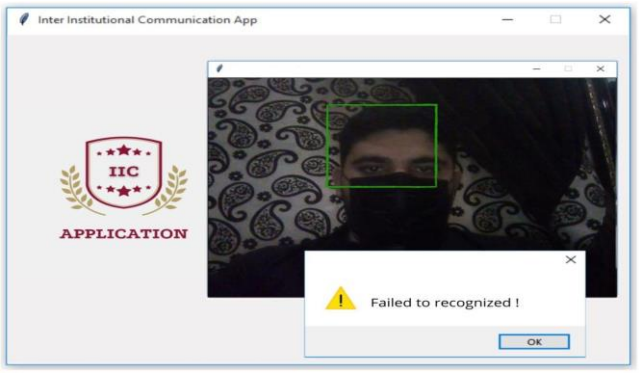

Figure 3.6: Facial Detection. When a face was not recognized, a message was displayed on the screen of a developed inter-institutional communication application.

The use of more than one authentication is to secure the inter-institutional communication system. However, the authentication process like face recognition and detection is required every time the application is re-opened. Once the authentication process is completed, the home page of the inter-institutional communication application is opened (Figure 3.7).

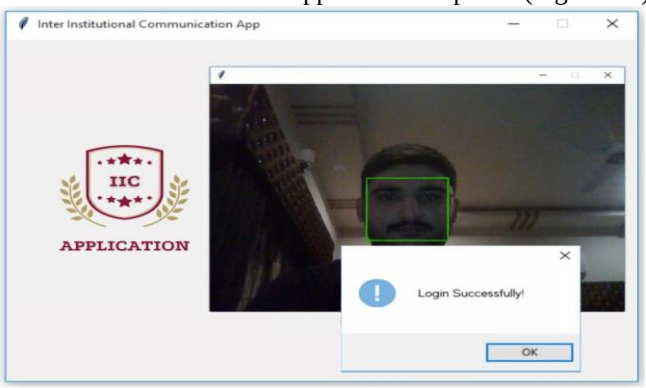

Figure 3.7: Facial Detection. Screenshot of a developed inter-institutional communication application displaying a success message after a successful face recognition.

When the home page of the inter-institutional communication application is opened, it shows the many notifications along with date, department, and subject from the administration side and from the department side (Figure 3.8). There are also many options which show the profile of registered people who are using the application through their registered email. After that, there is an issue notification option in which notification is issued to the departments or administration side. After that, the view notification option is used when viewing any notification that comes from the department side or administration side. After that, the log out option is used for registered people who logged into the application. By using this option, the registered person is automatically logged out from the application and the login window appears again for re-login.

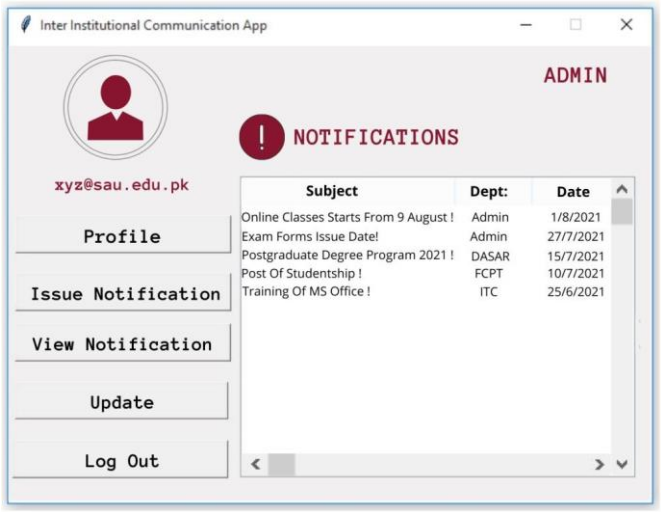

Figure 3.8: The home screen of an inter-institutional communication application that has been developed.

When the issue notification option is selected, then the issue notification window is opened on screen and shows many options for issue notification. First select the to option to enter the notification reciever's designation and then select the department box where you have to send the notification in which department. The selection of department is completed, then the outward box is selected to enter the outward number for the notification. After that, the date box is selected, when the date is entered successfully, tick the checkbuttons which show in the CC box where you have to send the copy of that notification (Figure 3.9).

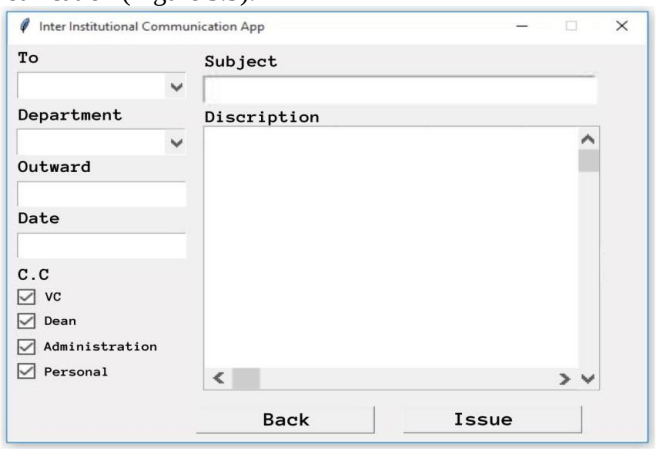

Figure 3.9: Issue Notification Option Screen of developed inter-institutional communication application.

In the subject box (Figure 3.10), the notification's outline is entered in the subject box, which is shown on the main window where all notifications are shown with their date and department. After the subject box, in the description box, the details of the notification are entered. When the notification is selected, all the details which are given in the description are shown on the view screen with the date and its outward number. When all options are completely selected and correctly filled, then the notification is successfully issued (Figure 3.11).

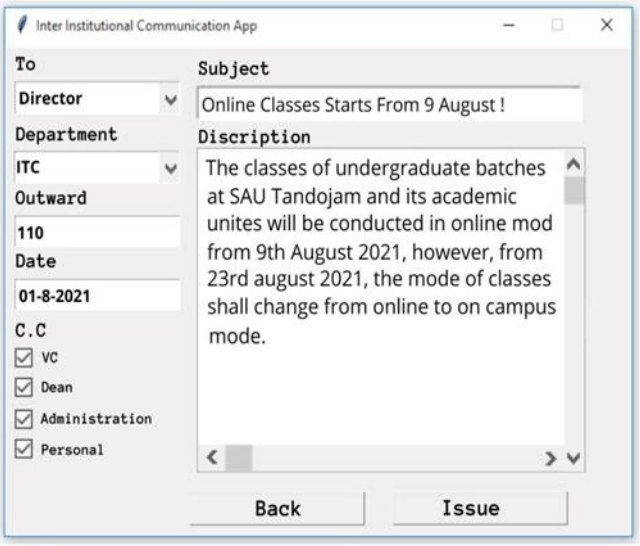

Figure 3.10: Issuing Notification in a developed inter-institutional communication application

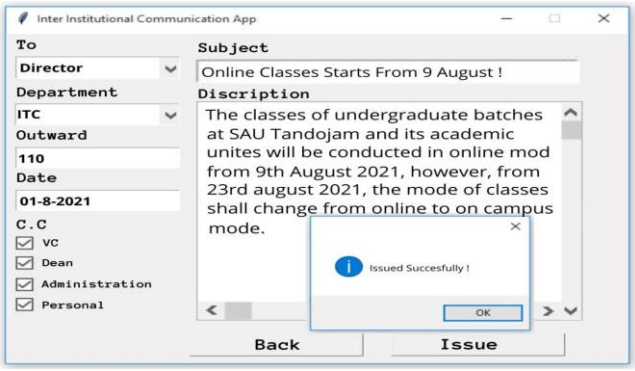

Figure 3.11: success message shown when notification is issued in a developed, inter-institutional communication application

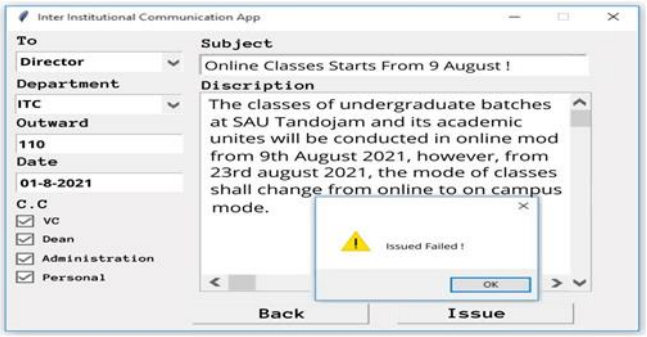

Figure 3.12: Failure message displayed when a notification is issued in an inter-institutional communication application that has been developed.

In (Figure 3.12), when the notification's outward is the same as the older one, it is issued an error. Notification with the same outward will not proceed further.

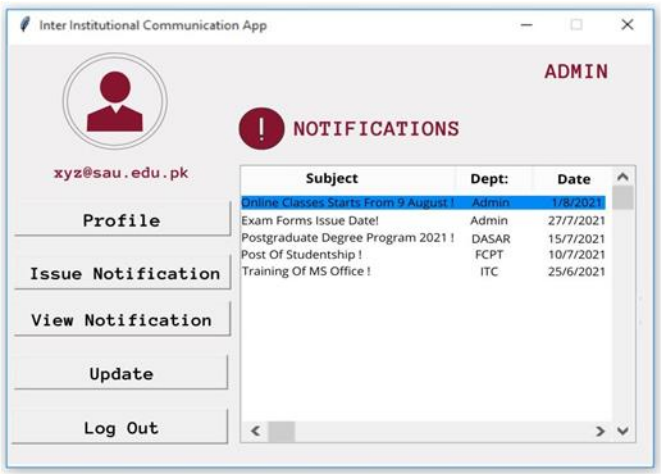

Figure 3.13: A list of notifications from the developed inter-institutional communication application is shown.

Figure 3.14: Sample Notification Issued in Inter-Institutional Communication Application.

In Figure 3.13, when we select a notification from the home page to view the notification, we select the notification, press the view notification button, and the notification will proceed and open the view notification window. In (Figure 3.14), the notification window is opened and all the details of the notification, along with the date, outward and all the description that were entered during the issue notification process, can be viewed clearly.

3.4 STRUCTURE OF THE BLOCKCHAIN

To keep the integrity and security of communication, the data was stored in the blockchain structure. Here, in our case, all the notifications were stored in the blockchain structure. Each notification was stored in a different block, and all the blocks were connected with their next and previous blocks. Each block consisted of the data (notification), timestamps (the time at which data was stored in the block), previous hash (hash value of the previous block), current hash (hash value of the current block) (Figure 3.15).

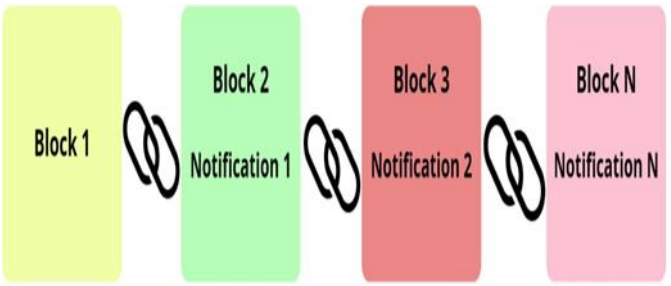

Figure 3.15: Blockchain diagram for proposed inter-institutional communication model.

4 RESULTS

The empirical results of inter-institutional communication were evaluated by two different tests, which were conducted at Sindh Agriculture University Tandojam, at different times and dates. The results are as follows:

4.1 RESULTS OF 1st TEST

In the first test of the inter- Institutional communication application, which was conducted in the first week of July 2021, 6 faculties were invited, from which 2 of the could not participate because of their busy schedule and remaining the 4-department participated (Table 4.1).

Table 4. 1: Participants of 1st test of inter-institutional communication application.

S. No	Name of The Department /Faculty	User of the department
1	ITC	Co-Ordinator
2	ADMINISTRATION	Registrar
3	FCPT	Dean
4	ITC	Director

Since there were 4 departments participate, each of which included different stakeholders. In the Faculty of Crop Protection, Coordinator of the faculty was using the application however for Faculty of agriculture Engineering, Chairman of the department of the Farm Power Machineries was using. For the ITC and FCPD, Undergraduate Coordinators were using the application. For the testing purpose coordinator of ITC issues 2 notifications to the administration and 1 notification for general purposed which were visible to everyone. Faculty of agricultural engineering issued total of 4 notifications among which 2 of those were issued to ITC and remaining two were for everyone. (Figure 4.1)

S. No	Name of the Department /Faculty	User of the department
1	FAE	Co-Ordinator
2	IFST	Co-Ordinator
3	ITC	Co-Ordinator
4	ADMINISTRATION	Registrar
5	FCPD	Co-Ordinator

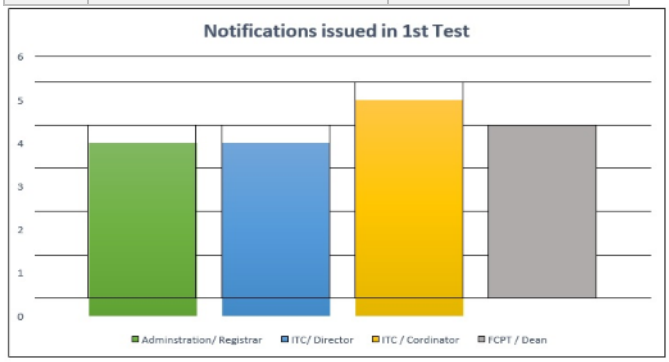

Figure 4.1: Notifications issued in the 1st test of the inter-institutional communication application.

In the first test, a total of 13 notifications were issued by all participating departments and faculties, i.e., the Information Technology Centre, the Faculty of Agricultural Engineering, the Faculty of Crop Protection, and the Administration. Since the data was stored in the blockchain structure in order to make the data integrated and secure, a total of 14 blocks were created. The first block was the genesis block, which is always the first block of every blockchain. These 14 blocks were connected with their next and previous blocks (Figure 4.2).

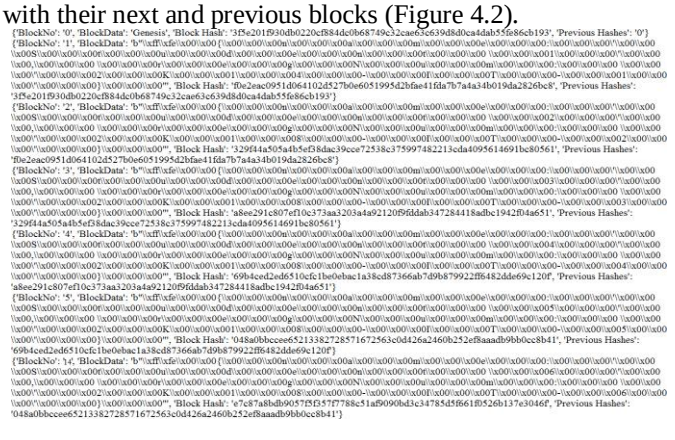

Figure 4. 2: Blockchain structure formed during the 1st test of inter-institutional communication application.

4.2 RESULTS OF 2nd TEST

The 2nd test of the intern-institutional communication application was conducted in the last week of July 2021, 5 faculties were invited and all of the 5-department participated, listof the departments faculties can be seen in the Table 4.2. This test was supposed to be criticaltest because the main motive of the test was to detect and recognize the Fraud and unauthenticity. In this test the different users were asked to use the application despite of its registered stakeholders

Table 4. 2: Participants of 2nd test of inter-institutional communication application

Since the 5 users were using the application but only 4 of them were successfully authenticated and authorized and 1 of them was failed in facial authentication and recognition and he/she could not use the application and our system successfully proved to be secure (Figure 4.3)

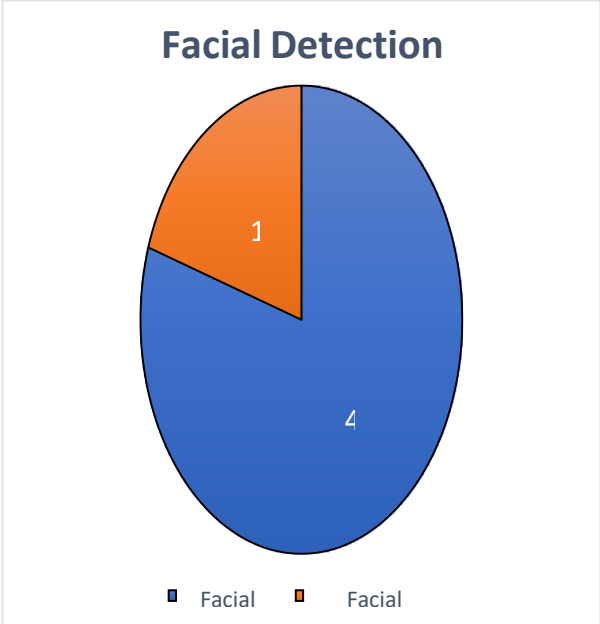

Figure 4.3: Ratio of biometric recognition and failure entities during 1st test of inter-institutional communication application

Since there were 5 users of departments/faculties participated, each of which included different stakeholders. In the Faculty of Crop Production, Coordinator of the faculty was using the application, for Department of Information Technology Center, Co-Ordinator of the department was using. For the Administration, Registrar was using the application. In the Faculty of Agriculture Engineering, Coordinator of the faculty was using the application however for Department of Food and Science Technology, Co-Ordinator of the department was using the inter-institutional communication application. For the testing purpose Co-Ordinator of Information Technology Center issues 4 notifications to the administration and 2 notifications for general purpose which were visible to everyone. The Coordinator of Faculty of Agriculture Engineering was issued total of 4 notifications among which 2 of those were issued to Information Technology Center and 1 of them issued to administration and remaining 1 were for everyone. The Administration was issued total 2 notifications for general purpose which were visible to everyone. The Co-Ordinator of Department of Crop Production was issued total 2 notifications 1 of them issued to administration and remaining 1 were for everyone and the user of last department i.e. Institute of Food science and technology, which was failed in Facial detection and recognition, could not issue or read the notification because his/her portal could not be opened Figure 4.4.

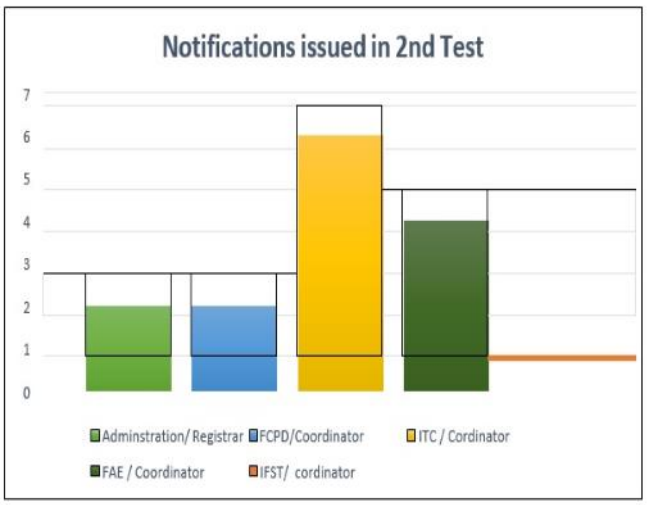

Figure 4.4: Notifications issued in the 2nd test of inter-institutional communicationapplication.

In the Second test total of 14 notifications were issued by all participating departments/faculties i.e., Information Technology Centre, Institute of Food science and technology, Faculty of Agricultural Engineering, Faculty of Crop Production, and the Administration. Since the data was stored in the blockchain structure in order to make the data integrated and secure, total of 15 blocks were created, first block was genesis block which is always the first block of every blockchain, these all 15 blocks were connected with its next and previous block (Figure 4.5).

{'BlockNo': '0', 'BlockData': 'Genesis', 'Block Hash': '3f5e201f930db0220cf884dc0b68749c32cae63c639d8d0ca4dab55fe86cb193', 'Previous Hashes': '0'}
{'BlockNo': '1', 'BlockData': 'b"\\xff\\xfe\\x00\\x00{\\x00\\x00\\x00n\\x00\\x00\\x00a\\x00\\x00\\x00m\\x00\\x00\\x00e\\x00\\x00\\x00:\\x00\\x00\\x00\'\\x00\\x00
\\x00S\\x00\\x00\\x00f\\x00\\x00\\x00o\\x00\\x00\\x00d\\x00\\x00\\x00 \\x00\\x00\\x00a\\x00\\x00\\x00n\\x00\\x00\\x00d\\x00\\x00\\x00 \\x00\\x00\\x00\\x00 \\x00\\x00\\x00\\x00 \\x00\\x00\\x00\\x00 \\x00\\x00\\x00\\x00 \\x00\\x00\\x00\\x00
\\x00,\\x00\\x00\\x00 \\x00\\x00\\x00n\\x00\\x00\\x00o\\x00\\x00\\x00 \\x00\\x00\\x00g\\x00\\x00\\x00N\\x00\\x00\\x00a\\x00\\x00\\x00m\\x00\\x00\\x00:\\x00\\x00\\x00 \\x00\\x00
\\x00\\'\\x00\\x00\\x00\\x02\\x00\\x00\\x00K\\x00\\x00\\x00\\x01\\x00\\x00\\x00\\x04\\x00\\x00\\x00-\\x00\\x00\\x00\\x01\\x00\\x00\\x00\\x07\\x00\\x00\\x00-\\x00\\x00\\x00\\x01\\x00\\x00
\\x00\\'\\x00\\x00\\x00\\x01}\\x00\\x00\\x00\\'", 'Block Hash': 'f0e2eac0951d064102d527b0e6051995d2bfae41fda7b7a4a34b019da2826bc8', 'Previous Hashes':
'3f5e201f930db0220cf884dc0b68749c32cae63c639d8d0ca4dab55fe86cb193'}
{'BlockNo': '2', 'BlockData': 'b"\\xff\\xfe\\x00\\x00{\\x00\\x00\\x00n\\x00\\x00\\x00a\\x00\\x00\\x00m\\x00\\x00\\x00e\\x00\\x00\\x00:\\x00\\x00\\x00\'\\x00\\x00
\\x00S\\x00\\x00\\x00f\\x00\\x00\\x00o\\x00\\x00\\x00d\\x00\\x00\\x00 \\x00\\x00\\x00a\\x00\\x00\\x00n\\x00\\x00\\x00d\\x00\\x00\\x00 \\x00\\x00\\x00\\x02\\x00\\x00\\x00\'\\x00\\x00
\\x00,\\x00\\x00\\x00 \\x00\\x00\\x00n\\x00\\x00\\x00o\\x00\\x00\\x00 \\x00\\x00\\x00g\\x00\\x00\\x00N\\x00\\x00\\x00a\\x00\\x00\\x00m\\x00\\x00\\x00:\\x00\\x00\\x00 \\x00\\x00
\\x00\\'\\x00\\x00\\x00\\x02\\x00\\x00\\x00K\\x00\\x00\\x00\\x01\\x00\\x00\\x00\\x08\\x00\\x00\\x00-\\x00\\x00\\x00\\x01\\x00\\x00\\x00\\x07\\x00\\x00\\x00-\\x00\\x00\\x00\\x02\\x00\\x00
\\x00\\'\\x00\\x00\\x00\\x01}\\x00\\x00\\x00\\'", 'Block Hash': '329f44a505a4b5ef38dac39cce72538c375997482213cda4095614691bc80561', 'Previous Hashes':
'f0e2eac0951d064102d527b0e6051995d2bfae41fda7b7a4a34b019da2826bc8'}
{'BlockNo': '3', 'BlockData': 'b"\\xff\\xfe\\x00\\x00{\\x00\\x00\\x00n\\x00\\x00\\x00a\\x00\\x00\\x00m\\x00\\x00\\x00e\\x00\\x00\\x00:\\x00\\x00\\x00\'\\x00\\x00
\\x00S\\x00\\x00\\x00f\\x00\\x00\\x00o\\x00\\x00\\x00d\\x00\\x00\\x00 \\x00\\x00\\x00a\\x00\\x00\\x00n\\x00\\x00\\x00d\\x00\\x00\\x00 \\x00\\x00\\x00\\x03\\x00\\x00\\x00\'\\x00\\x00
\\x00,\\x00\\x00\\x00 \\x00\\x00\\x00n\\x00\\x00\\x00o\\x00\\x00\\x00 \\x00\\x00\\x00g\\x00\\x00\\x00N\\x00\\x00\\x00a\\x00\\x00\\x00m\\x00\\x00\\x00:\\x00\\x00\\x00 \\x00\\x00
\\x00\\'\\x00\\x00\\x00\\x02\\x00\\x00\\x00K\\x00\\x00\\x00\\x01\\x00\\x00\\x00\\x08\\x00\\x00\\x00-\\x00\\x00\\x00\\x01\\x00\\x00\\x00\\x07\\x00\\x00\\x00-\\x00\\x00\\x00\\x03\\x00\\x00
\\x00\\'\\x00\\x00\\x00\\x01}\\x00\\x00\\x00\\'", 'Block Hash': 'a8ee291c807ef10c373aa3203a4a92120f9fddab347284418adbc1942ff04a651', 'Previous Hashes':
'329f44a505a4b5ef38dac39cce72538c375997482213cda4095614691bc80561'}
{'BlockNo': '4', 'BlockData': 'b"\\xff\\xfe\\x00\\x00{\\x00\\x00\\x00n\\x00\\x00\\x00a\\x00\\x00\\x00m\\x00\\x00\\x00e\\x00\\x00\\x00:\\x00\\x00\\x00\'\\x00\\x00
\\x00S\\x00\\x00\\x00f\\x00\\x00\\x00o\\x00\\x00\\x00d\\x00\\x00\\x00 \\x00\\x00\\x00a\\x00\\x00\\x00n\\x00\\x00\\x00d\\x00\\x00\\x00 \\x00\\x00\\x00\\x04\\x00\\x00\\x00\'\\x00\\x00
\\x00,\\x00\\x00\\x00 \\x00\\x00\\x00n\\x00\\x00\\x00o\\x00\\x00\\x00 \\x00\\x00\\x00g\\x00\\x00\\x00N\\x00\\x00\\x00a\\x00\\x00\\x00m\\x00\\x00\\x00:\\x00\\x00\\x00 \\x00\\x00
\\x00\\'\\x00\\x00\\x00\\x02\\x00\\x00\\x00K\\x00\\x00\\x00\\x01\\x00\\x00\\x00\\x08\\x00\\x00\\x00-\\x00\\x00\\x00\\x01\\x00\\x00\\x00\\x07\\x00\\x00\\x00-\\x00\\x00\\x00\\x04\\x00\\x00
\\x00\\'\\x00\\x00\\x00\\x01}\\x00\\x00\\x00\\'", 'Block Hash': '69b4ced2ed6510cfc1be0ebac1a38cd87366ab7d9b879922ff6482dde69c120f', 'Previous Hashes':
'a8ee291c807ef10c373aa3203a4a92120f9fddab347284418adbc1942ff04a651'}
{'BlockNo': '5', 'BlockData': 'b"\\xff\\xfe\\x00\\x00{\\x00\\x00\\x00n\\x00\\x00\\x00a\\x00\\x00\\x00m\\x00\\x00\\x00e\\x00\\x00\\x00:\\x00\\x00\\x00\'\\x00\\x00
\\x00S\\x00\\x00\\x00f\\x00\\x00\\x00o\\x00\\x00\\x00d\\x00\\x00\\x00 \\x00\\x00\\x00a\\x00\\x00\\x00n\\x00\\x00\\x00d\\x00\\x00\\x00 \\x00\\x00\\x00\\x05\\x00\\x00\\x00\'\\x00\\x00
\\x00,\\x00\\x00\\x00 \\x00\\x00\\x00n\\x00\\x00\\x00o\\x00\\x00\\x00 \\x00\\x00\\x00g\\x00\\x00\\x00N\\x00\\x00\\x00a\\x00\\x00\\x00m\\x00\\x00\\x00:\\x00\\x00\\x00 \\x00\\x00
\\x00\\'\\x00\\x00\\x00\\x02\\x00\\x00\\x00K\\x00\\x00\\x00\\x01\\x00\\x00\\x00\\x08\\x00\\x00\\x00-\\x00\\x00\\x00\\x01\\x00\\x00\\x00\\x07\\x00\\x00\\x00-\\x00\\x00\\x00\\x05\\x00\\x00
\\x00\\'\\x00\\x00\\x00\\x01}\\x00\\x00\\x00\\'", 'Block Hash': '048a0bbccee6521338272857l672563c0d426a2460b252ef8aaadb9bb0cc8b41', 'Previous Hashes':
'69b4ced2ed6510cfc1be0ebac1a38cd87366ab7d9b879922ff6482dde69c120f'}
{'BlockNo': '15', 'BlockData': 'b"\\xff\\xfe\\x00\\x00{\\x00\\x00\\x00n\\x00\\x00\\x00a\\x00\\x00\\x00m\\x00\\x00\\x00e\\x00\\x00\\x00:\\x00\\x00\\x00\'\\x00\\x00
\\x00S\\x00\\x00\\x00f\\x00\\x00\\x00o\\x00\\x00\\x00d\\x00\\x00\\x00 \\x00\\x00\\x00a\\x00\\x00\\x00n\\x00\\x00\\x00d\\x00\\x00\\x00 \\x00\\x00\\x00\\x06\\x00\\x00\\x00\'\\x00\\x00
\\x00,\\x00\\x00\\x00 \\x00\\x00\\x00n\\x00\\x00\\x00o\\x00\\x00\\x00 \\x00\\x00\\x00g\\x00\\x00\\x00N\\x00\\x00\\x00a\\x00\\x00\\x00m\\x00\\x00\\x00:\\x00\\x00\\x00 \\x00\\x00
\\x00\\'\\x00\\x00\\x00\\x02\\x00\\x00\\x00K\\x00\\x00\\x00\\x01\\x00\\x00\\x00\\x08\\x00\\x00\\x00-\\x00\\x00\\x00\\x01\\x00\\x00\\x00\\x07\\x00\\x00\\x00-\\x00\\x00\\x00\\x06\\x00\\x00
\\x00\\'\\x00\\x00\\x00\\x01}\\x00\\x00\\x00\\'", 'Block Hash': 'e7c87a8bdb9057ff3f57f7788c51af9090bd3c34785d5f661f0526b137e3046f', 'Previous Hashes':
'048a0bbccee6521338272857l672563c0d426a2460b252ef8aaadb9bb0cc8b41'}

Figure 4. 5: Blockchain structure formed during the 2nd test of inter-institutionalcommunication application.

5. CONCLUSION

This research concluded that Artificial Intelligence and Blockchain technologies were used to share official information by designing a secure inter-institutional model that was validated through empirical results in which two tests were conducted. Each of the tests consisted of a different number of entities and different scenarios. This model proved to be a secure model, which caused an increase in the confidentiality and integrity of official information.

6. REFRENCES

[1]. Sharma, Y., Balamurugan, B., Snegar, N., & Ilavendhan, A. (2021). How IoT, AI, and Blockchain Will Revolutionize Business. In Blockchain, Internet of Things, and Artificial Intelligence (pp. 235-255). Chapman and Hall/CRC.

[2]. Harris, J. D., & Waggoner, B. (2019, July). Decentralized and collaborative AI on blockchain. In 2019 IEEE International Conference on Blockchain (Blockchain) (pp. 368-375). IEEE.

[3]. Schenk, E.; Schaeffer, V.; Pénin, J. Blockchain and the Future of Open Innovation Intermediaries: The Case of Crowdsourcing Platforms. In Managing Digital Open Innovation; World Scientific Publishing Co.: Singapore, 2020.

[4]. Rico-Bautista, D., Medina-Cardenas, Y., Coronel-Rojas, L. A., Cuesta-Quintero, F., Maestre-Gongora, G., & Guerrero, C. D. (2021). Smart University: Key Factors for an Artificial Intelligence Adoption Model. Advances and Applications in Computer Science, Electronics and Industrial Engineering, 1307, 153-166.

[5]. Gupta, R., Tanwar, S., Al-Turjman, F., Italiya, P., Nauman, A., & Kim, S. W. (2020). Smart contract privacy protection using ai in cyber-physical systems: Tools, techniques and challenges. IEEE Access, 8, 24746-24772.

[6]. Hu, Y. H. (2021). Effects and acceptance of precision education in an AI-supported smart learning environment. Education and Information Technologies, 1-25.

[7]. Veselov, G., Tselykh, A., Sharma, A., & Huang, R. (2021). Applications of Artificial Intelligence in Evolution of Smart Cities and Societies. Informatica, 45(5).

[8]. J. Mendling, I. Weber, W. M. P. Aalst, J. v. Brocke, C. Cabanillas, F. Daniel, S. Debois, C. Di Ciccio, M. Dumas, S. Dustdar, A. Gal, L. García-Bañuelos, G. Governatori, R. Hull, M. La Rosa, H. Leopold, F. Leymann, J. Recker, M. Reichert, and L. Zhu, "Blockchains for business process management - challenges and opportunities," ACM Transactions on Management Information Systems, vol.In press, accepted, 01 2018.

[9].Akhrif, O., El Idrissi, Y. E. B., & Hmina, N. (2018, October). Smart university: SOC- based study. In Proceedings of the 3rd International Conference on Smart City Applications (pp. 1-6).

[10]. Raja, G., Manaswini, Y., Vivekanandan, G. D., Sampath, H., Dev, K., & Bashir, A. K. (2020, July). AI-powered blockchain-a decentralized secure multiparty computation protocol for IoV. In IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) (pp. 865-870). IEEE.

[11]. Heister, S., & Yuthas, K. (2021). How Blockchain and AI Enable Personal Data Privacy and Support Cybersecurity. In Blockchain Potential in AI. IntechOpen.

[12]. Marwala, T., & Xing, B. (2018). Blockchain and artificial intelligence. arXiv preprint arXiv:1802.04451.

[13]. Kariapper, R. K. A. R., Nafrees, A. C. M., Razeeth, M. S., & Pirapuraj, P. (2020). Emerging Smart University using various Technologies: A Survey Analysis. Test Eng. Manag. Mattingley Publ. Co., Inc. ISSN, 83, 17713-17723.

[14]. Hung, N. Q., Phung, T. K., Hien, P., & Thanh, D. N. H. (2021). AI and Blockchain: potential and challenge for building a smart E-Learning system in Vietnam. In IOP Conference

Series: Materials Science and Engineering (Vol. 1022, No. 1, p. 012001). IOP Publishing.
[15]. Bodkhe, Umesh, Sudeep Tanwar, Karan Parekh, Pimal Khanpara, Sudhanshu Tyagi, Neeraj Kumar, and Mamoun Alazab. "Blockchain for industry 4.0: A comprehensive review." IEEE Access 8 (2020): 79764-79800.
[16]. B. Sánchez-Torres, J. A. Rodríguez-Rodríguez, D. W. Rico-Bautista, and C. D. Guerrero, "Smart Campus: Trends in cybersecurity and future development," Rev. Fac. Ing., vol. 27, no. 47, pp. 93–101, 2018.
[17]. S. Rajebhosale, S. Choudhari, S. Patil, A. Vyavahare, S. Khabiya, and A. Professor, "SMART CAMPUS-An Academic Web Portal with Android Application," Int. Res. J. Eng. Technol., 2016.
[18]. Abougalala, R. A., Amasha, A., Areed, M. F., Alkhalaf, S., & Khairy, D. (2020). Blockchain- enabled smart university: A framework. Journal of Theoretical and Applied Information Technology, 98(17), 3531-3543.
[19]. Nawaz, A., Gia, T. N., Queralta, J. P., & Westerlund, T. (2019, November). Edge AI and blockchain for privacy-critical and data-sensitive applications. In 2019 Twelfth International Conference on Mobile Computing and Ubiquitous Network (ICMU) (pp. 1-2). IEEE.
[20]. Pisa, M. and Juden, M., 2017. Blockchain and economic development: Hype vs. reality. Center for Global Development Policy Paper, 107, p.150.
[21]. W. Villegas-Ch, X. Palacios-Pacheco, and S. Luján-Mora, "Application of a smart city model to a traditional university campus with a big data architecture: A sustainable smart campus," Sustain., 2019.
[22]. M. Mettler, "Blockchain Technology in Healthcare: The Revolution Starts Here," Proc. IEEE 18th Int'l Conf. e-Health Networking, Applications and Services (Healthcom 16), 2016, doi:10.1109/HealthCom.2016.7749510
[23]. P. Fraga-Lamas and T. M. Fernández-Caramés, "A review on blockchain technologies for an advanced and cyber-resilient automotive industry," IEEE Access, vol. 7, pp. 17578– 17598, 2019.
[24]. Seebacher, S., & Schüritz, R. (2017). Blockchain technology as an enabler of service systems: A structured literature review, In Exploring Services Science, vol. 279 of Lecture Notes in Business Information Processing, pp. 12-23, Springer International Publishing, Cham, 2017.
[25]. P. Williams, "Does Competency-Based Education with Blockchain Signal a New Mission for Universities?" Journal of Higher Education Policy and Management, Vol. 41, No. 1, 2019, pp. 104-117.
[26]. Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Communications Surveys & Tutorials, 18(3), 2084- 2123.
[27]. A. Kamišalić, M. Turkanović, S. Mrdović, and M. Heričko, "A Preliminary Review of Blockchain-Based Solutions in Higher Education." In: L. Uden, D. Liberona, G. Sanchez, and S. Rodríguez-González, eds, Learning Technology for Education Challenges. LTEC 2019. Cham, Switzerland: Springer; April 2019, pp. 114124.
[28]. A. Ramachandran and D. Kantarcioglu, "Using Blockchain and Smart Contracts for Secure Data Provenance Management," 2017, arXiv preprint arXiv:1709.10000.
[29]. U. Javaid, M.N. Aman, and B. Sikdar, "Blockpro: Blockchain Based Data Provenance and Integrity for Secure IoT Environments," Proceedings of the 1st Workshop on Blockchain-Enabled Networked Sensor Systems, Association for Computing Machinery (China), November 4, 2018, pp. 13-18.
[30]. G. Khan, S. Jabeen, M.Z. Khan, M.U.G. Khan, and R. Iqbal, "Blockchain-Enabled Deep Semantic Video-to-Video Summarization for IoT Devices," Computers & Electrical Engineering, Vol. 81, 2020, art. 106524.
[31]. V. J. Morkunas, J. Paschen, and E. Boon, "How blockchain technologies impact your business model," Business Horizons, vol. 62, no. 3, pp. 295 – 306, 2019. [32]. T.M. Fernández-Caramés and P. FragaLamas, "Towards Next Generation Teaching, Learning, and Context-Aware Applications for Higher Education: A Review on Blockchain, IoT, Fog and Edge Computing Enabled Smart Campuses and Universities," Applied Sciences, Vol. 9, No. 21, 2019, art. 4479.
[33]. D. Lu, P. Moreno-Sanchez, Z. Zeryihun, S. Bajpayi, S. Yin, K. Feldman, J. Kosofsky, P. Mitra, and A. Kate, "Reducing Automotive Counterfeiting Using Blockchain: Benefits and Challenges," 2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON), IEEE (US) April 4-9, 2019, pp. 39-48.
[34]. K. Fan, S. Sun, Z. Yan, Q. Pan, H. Li, and Y. Yang, "A Blockchain-Based Clock Synchronization Scheme in IoT," Future Generation Computer Systems, Vol. 101, December 2019, pp. 524-533.