Cyber Security and Applications 1 (2023) 100005

Contents lists available at ScienceDirect

Cyber Security and Applications

journal homepage: http://www.keaipublishing.com/en/journals/cyber-security-and-applications/

An advanced and secure framework for conducting online examination using blockchain method

Md Rahat Ibne Sattar[a,*], Md. Thowhid Bin Hossain Efty[a], Taiyaba Shadaka Rafa[a], Tusar Das[a], Md Sharif Samad[a], Abhijit Pathak[a], Mayeen Uddin Khandaker[b,c,*], Md. Habib Ullah[d]

[a] Department of Computer Science and Engineering, BGC Trust University Bangladesh, Chattogram, Bangladesh
[b] Centre for Applied Physics and Radiation Technologies, School of Engineering and Technology, Sunway University, 47500 Bandar Sunway, Selangor, Malaysia
[c] Department of General Educational Development, Faculty of Science and Information Technology, Daffodil International University, DIU Rd, Dhaka 1341, Bangladesh
[d] Department of Physics, Faculty of Science and Technology, American International University-Bangladesh, Dhaka, 1229 Bangladesh

ARTICLE INFO

Keywords:
Online exam
IP-based login
Artificial intelligence
RDP
Blockchain
Proctor supervision

ABSTRACT

Nowadays, the online platform has been used by many educational institutions, to conduct tests, especially for secondary to tertiary level students. The most popular online test program is run by providing a user id and password to the candidates, and subsequently, they log in to the given web page to answer the questions. However, this system has a lot of bugs, the password can be misused followed by cheating in the test. This shows the importance of a secure system being implemented to avoid such a problem. This paper presents a blockchain framework that secures the online examination system. The proposed framework has been used to secure a data management system that connects to existing educational data. Institutions can simply compile their data history without requiring a copy from the central servers. The proposed blockchain framework improves data security and removes any potential cheating between users or third-party institutions that access applications and services. In this regard, this study provides a secured framework for conducting and evaluating subject tests to ensure consistency between student and server, and secure delivery of questionnaire from the server.

1. Introduction

During the Covid-19 pandemic, all educational institutions in Bangladesh are closed physically like the other countries in the world. As a result, more than four crore students in Bangladesh have been affected, and students have no other choice but to study online. Also, the examinations are conducted via an online platform. However, the proper evaluation of students learning via online examination has remained appalling. Specifically, some issues such as Fake Identity, Question Distribution, Common questions, Background Apps or Multiple Devices, Copy Answer-script, and Secure Result Publication have appeared as a significant concern. It becomes very necessary to solve those significant issues; if not, many students will lag in terms of quality education. Fortunately, in Bangladesh, the use of communication technology has grown significantly in recent years. In this regard, an advanced and secure framework for an online examination system is designed to enhance the efficacy of the online examination procedure for educational institutions such as schools, colleges, and universities in Bangladesh. The main perspective of this research work is to build a proper system to solve all major problems that students and teachers have been facing during the online examination. This study looks at the challenge of personal identity and unauthorised access of other users to the network using different clients.

The objectives of the study are to (i) Analyze the features of several online programs that perform online tests for a variety of purposes, and (ii) Develop a blockchain-based secure online examination system for educational institutions in Bangladesh.

It is expected that the proposed system can handle all operations from the beginning of IP-based login to block-chain-based result publication that makes the exam procedure more secure, user-friendly, time-saving, and effective.

2. Literature review

Cluskey et al. [1] studied the possible ways to take the online exam without having proctor supervision. The authors have discussed in detail the common cheating scenario that is adopted by the students, and how to prevent the students from cheating. They have suggested some techniques for developing an online testing plan and some online exam control procedures such as taking exams at one set time, using Respondus Lockdown Browser (RDL), verifying student ID, and so on. Tejra et al.

* Corresponding author.
E-mail addresses: rahat@bgctub.ac.bd (M.R.I. Sattar), mayeenk@sunway.edu.my (M.U. Khandaker).

https://doi.org/10.1016/j.csa.2022.100005
Received 10 April 2022; Received in revised form 4 June 2022; Accepted 10 August 2022
Available online 11 August 2022

[2] have proposed to use of Convolutional Neural Networks (CNN) to identify a student properly in an online exam by observing the student's movement. But the drawback of CNN is that it can't analyze the orientation and position of students and it also needs too much data to preview the result. Mukta et al. [3] have worked on the Fuzzy Logic Approach for Adaptive Test Sheet Generation in E-Learning. They suggested the use of an ambiguous method of assessing students' favorite tests in the e-learning area. Jung and Yeom [4] have discussed how someone can secure an online exam management system using group cryptography. They describe how the SECONE software system can help to build a secure online management system. However, it requires the use of high-quality webcams and a microphone, which is a drawback for the system. Liu and Fan [5] have introduced the terminology 'analytics' in evaluating the students' learning outcomes. According to the authors, the study of mathematics should be enabled in educational institutions to increase the understanding of student learning needs, and this may make a positive impact on learners' learning and progression. Monjitha and colleagues [6] have proposed a system in which the questionnaire's production manager selects a percentage of the complexity of the question. Depending on the percentage selection system, one can choose random questions that will satisfy the conditions. This program can also produce the paper according to the format provided by the administrator. After paper production, the paper will be saved in PDF format and emailed to colleges with a single click. Paul et al. [7] proposed how to design a question paper template according to the input requirements. Zhen and Su [8] proposed some methods for the face recognition system in this respect. The authors have described how neural networks (NN), Support Vector Machines (SVM), and Algebraic characterization can be utilized in face recognition systems. Jain and colleagues presented the importance of a blockchain network in the education system. They have developed an online examination system based on blockchain. They used the public blockchain platform 'Ethereal' and one of the best applications entitled 'Smart contracts' [9]. They have also compared the overall performance of the blockchain-based system with the cloud-based system. Lee and colleagues [10] proposed a system that categorizes the student's VFOA (visual focus of attention) data by capturing the head pose estimates and eye gaze estimates using state-of-the-art machine learning techniques. The examiner is alerted when the student wavers in his VFOA from the screen greater than X, a predefined threshold time; the application will save the person's data when his VFOA is off the screen and send it to the examiner to be manually checked and marked whether the student's action was attempted malpractice or just a momentary lapse in concentration. In "Digitalization Online Exam Cards in the Era of Disruption 5.0 using the DevOps Method" [11], the user behavior is detected using an online signature or displaying a student photo and fingerprint. They suggested Single Multiple Biometric detection techniques. In that study, they have detected student Online Signatures, Photos and Fingerprint, however, we are detecting student IP addresses, Face recognition, 360° Al view, and Noise detection method. In a study entitled "Utilizing webcam-based proctoring to deter misconduct in online exams", Hylton et al. [12] utilized a webcam-based proctoring procedure for online exams. They collected data from the results of online exams taken by participants as well as from the Web-based survey. They concluded that webcam-based proctoring deterred misconduct in online exams.

3. Proposed system

Because of the pandemic circumstances, educational institutions have been forced to shift the learning platforms to online. However, this shows some challenges, the major issue of adopting unethical steps by some students during the online examination. To solve such issues, this work proposes AI and Blockchain systems by considering the student identification, cheating scenario, and a secure result publication. The conceptual workflow of the proposed system is given in Fig. 1.

It is expected that it will create a new margin in the future educational system. Both student's devices and faculty agent's devices are connected through a server. All data from faculty members and students will be saved in the primary storage system through the database. Students' data can also be stored in the faculty agent's temporary storage through the database for a while. Every sector has a graphical user interface (GUI) to operate the system. From students' devices, the user identification interface data compilation interface date will be forwarded to the server's database.

4. Methodology

4.1. Working flowchart of evaluation system

The diagram in Fig. 2 illustrates the operational flow of the system. At first, a student will login to the system by using an IP address. After the login procedure, an AI-based face reorganization system alongside with 360° AI view and noise detection system will be enabled. Then the system will establish an RDP using an SSH connection. Subsequently, it will shuffle and specify each question for each IP/ID and set a specific time for each question to write the answer. After collecting all the answers script, it will create a database and check plagiarism for each script. If the answer script shows plagiarism of greater than seventy percent, then it will decide that the script has human interaction with another answer script, and it will simply forward the marks in the blockchain system. If it shows plagiarism of less than 70 percent, the system will forward the answer script to mark distribution. After that, it will forward the marks to the blockchain-based system. In this way, the system will come to an end.

4.2. Secure exam system control procedures (SESCP)

SESCP-A: Detect participant's IP for individual and establish that IP for future interaction. The student cannot change the device or any other person/network cannot interfere with their work.

SESCP-B: Recognize face using AI technology. It will detect face shape and the participant's movement. Parallel participants must submit a 360-panorama view. There, the AI system will detect electronic devices and human faces. YOLO algorithms are used in face detection. Its simple architecture increases the speed of detection, learning capabilities, and accuracy [13]. It is based on regression analysis. At first, it divides the taken images into N grids with an equal dimensional region of S x S. Each of these nodes is responsible for decision-making.

SESCP-C: Establishing a Remote Desktop Protocol to restrict background apps and, on the other side, traffic analyzers will work for any other network interaction. Consequently, the examinee prohibited using his device to interact with any other topic.

SESCP-D: The system will encrypt, break, and shuffle the whole question into a small section, generate a unique hash, and distribute that hash each into a specific IP. There will be a fixed time frame for each part of the question.

SESCP-E: The participant will have to provide the public key to the system. Then, the system will decrypt the question for individuals and collect the answer script on time.

SESCP-F: In this section, the system will make a database. Each answer script will be in the same database where the system will check for plagiarism for each answer- script. The paraphrasing tool is used to check plagiarism. It is a python-based tool that uses synonym usage, changing the grammatical structure, and changing part of speech as a technique. Semantic-based method, Grammar-based method, Grammar semantics hybrid method, and Clustering techniques are also used to check plagiarism. [14]

SESCP-G: This section will define plagiarism and eliminate answer scripts. We want human interactions here. Answer scripts having plagiarism of seventy percent or more will be forwarded to the teacher. They will judge and control those answer scripts for future procedures.

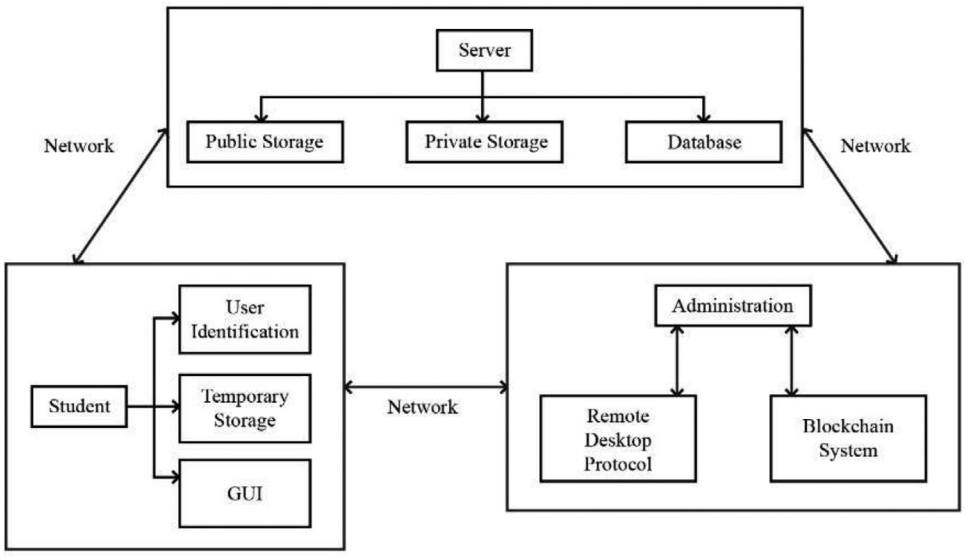


Fig. 1. Conceptual Framework of the Proposed System.

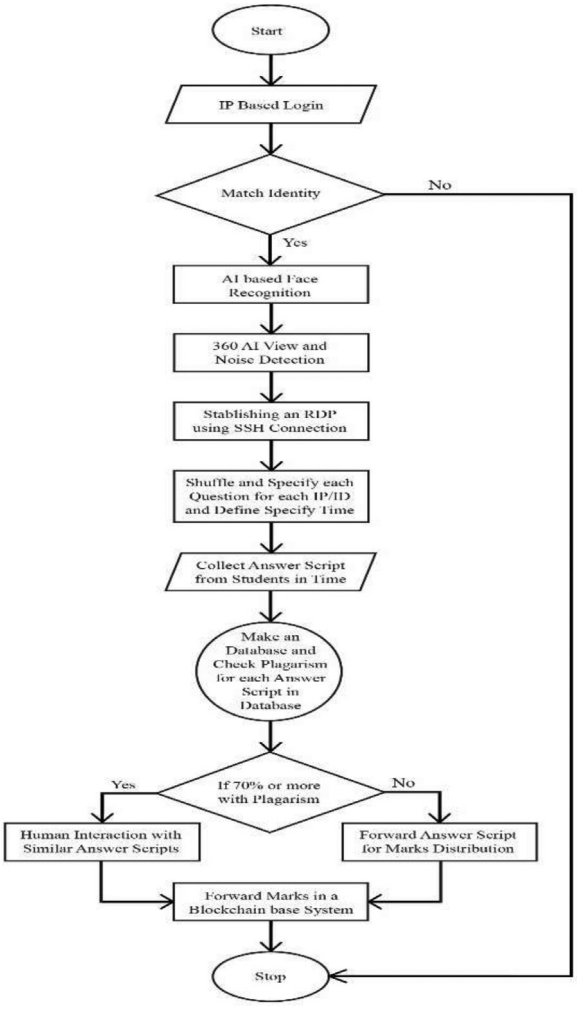


Fig. 2. Flowchart of the proposed system.

And, the rest of the answer script will be forwarded for marks distributions.

SESCP-H: The marks will be stored in a blockchain-based system to ensure security.

4.3. Blockchain implementation on marks distribution

Blockchain is a written posted database, and/or a computer database of any exchange, contracts - which should be freely recorded. One of the great features of Blockchain is that this computerized database is open with a few large PC numbers and will no doubt be stored in a single location. The most uplifting part of the square series is that it dramatically reduces the potential effects of the information break. Interestingly, with standard equitable processes, various shared duplicates of the same knowledge base make it difficult to pay for information attacks or digital attacks. With all the high-security features of the robbery, the establishment of square chains can change the diversity of business and make the forms smarter, safer, more straightforward, and more efficient compared to the standard business forms.

- The data is kept in JSON format, which is suitable to implement and easy to read. The data is kept in a block containing multiple data. Multiple blocks are added to determine others via fingerprinting.
- The fingerprinting is accomplished by employing hash and, to be precise, using the SHA256 hashing algorithm. Each block includes its own hash and the previous function's hash so that the system cannot be tampered.
- This fingerprinting is utilized to chain the blocks jointly. Every block is connected to the previous block, including its hash and the next block by giving its hash.
- The mining of the new block is accomplished by successfully discovering the solution to the proof of work. The proof of work must be hard to get manipulated to make mining challenges.
- After mining the block correctly, the block will be counted in the chain.
- After mining several blocks, the chain's validity must be restricted to prevent tampering with the blockchain.
- The web app is made with Flask.

Blockchain/DLT are the structure block of the "internet of value" and allow the recording of relations and transfer of "value" peer-to-peer, without a requirement for a centrally corresponding entity. "Value" directs to any record of asset license and license of specific information Fig. 4.

We use layer 1 blockchain scalability solutions for scalability, including sharding, segregated witness (SEGWIT), and hard forking. Layer 1 solutions focus on improving the blockchain network's core features and traits, such as enhancing the block size limit or decreasing the block verification time. Layer-1 solutions demand modifications in the codebase

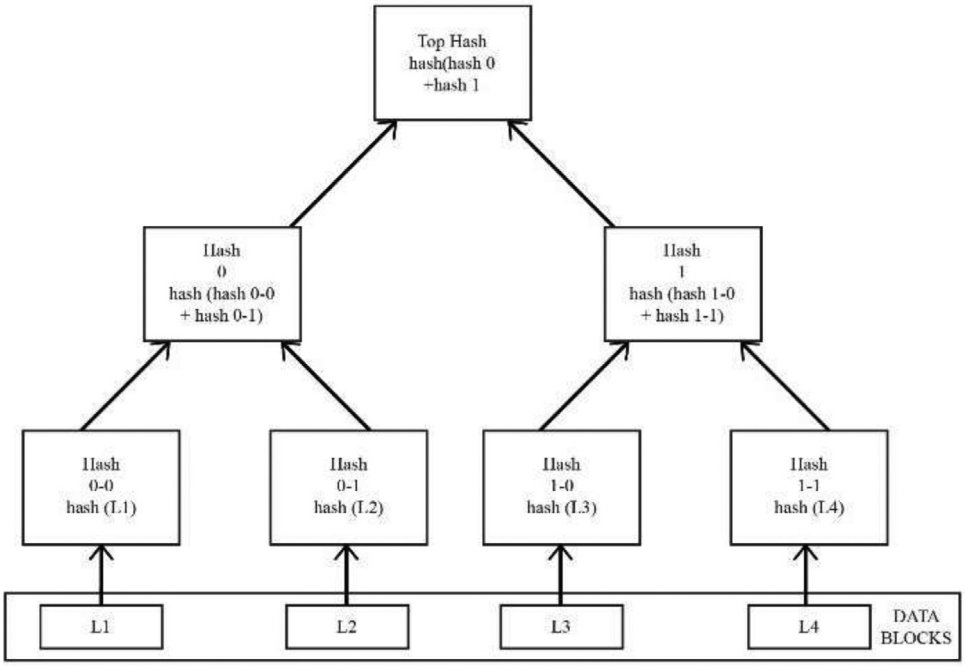


Fig. 3. Structure of the Blockchain technology.

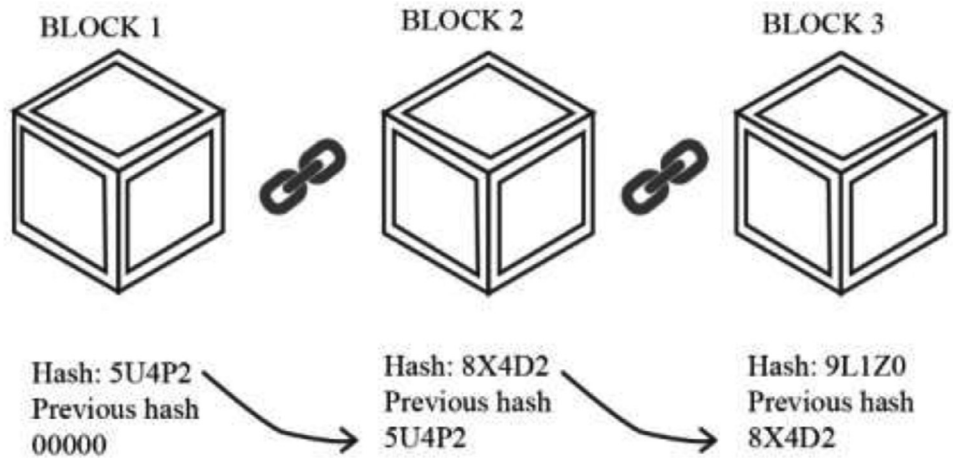


Fig. 4. Structure of data in the Blockchain technology.

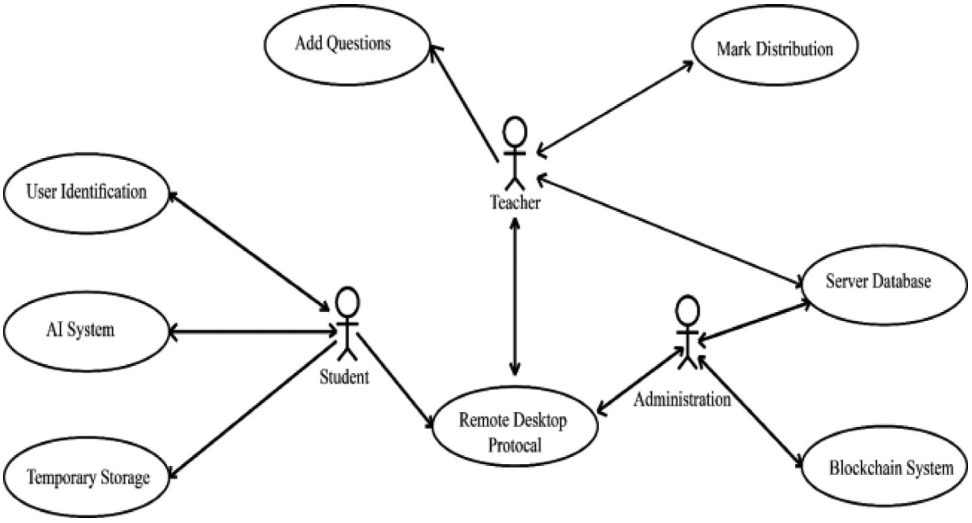
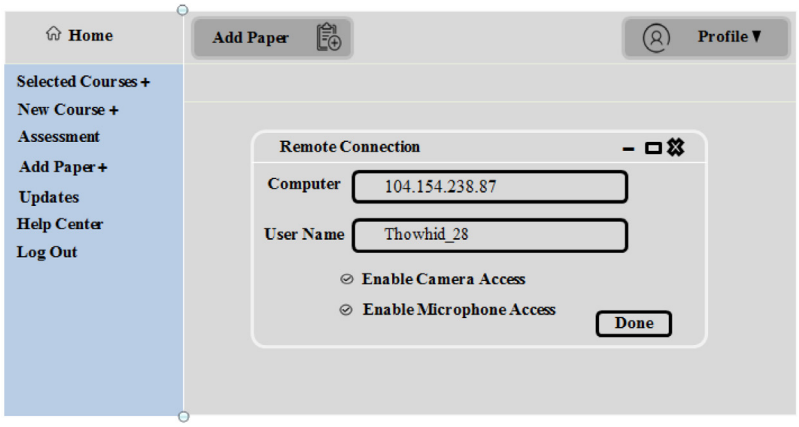
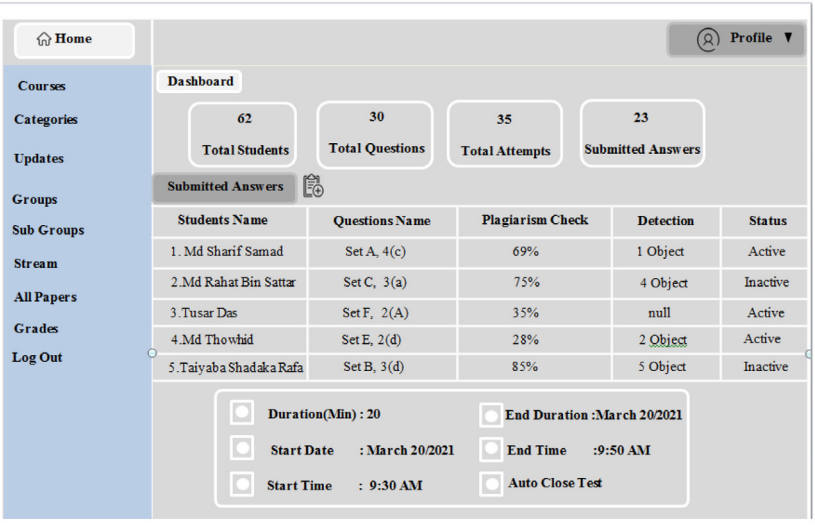


Fig. 5. User Interaction Diagram.



(a)



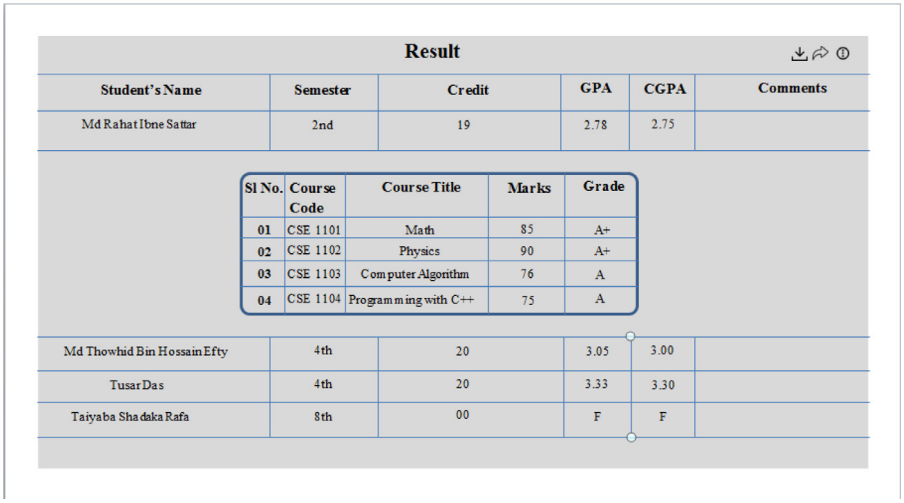


Fig. 6. Snapshots of the proposed system; (a) Student panel (b) Teacher panel and result panel.

of the leading blockchain network. Hence, layer 1 solutions are correspondingly guided as on-chain scaling solutions.

4.4. User interaction

The diagram illustrates the interaction system Fig. 5.

The user interaction diagram (Fig. 5) has three types of users, students, teachers, and administrators. Teachers distribute marks, add questions to the system, and can interact with the server database too. On the other side, students interact with the system through user identification protocol, AI-based system, and temporary storage. Moreover, the administrator directly interacts with the server database, marks distribution protocol, and blockchain-based system. Both students, teachers, and administrators interact with RDP (Remote desktop Protocol).

5. Results and future scope

Online exams range from MCQs, fill-in-the-blanks, checkboxes to short answers, long answers (that need to be evaluated by the teacher separately), coding simulators, case studies, etc. The education system is constantly evolving as well as its components. Here we present a few snapshots of our system Fig. 6.

In an online test, candidates should answer the questions within the prescribed time. The test window collapses when the test is over, and facilities receive real-time reports. The proposed automated system may scrutinize the answer scripts thoroughly and provide results in the shortest possible time. The testers checked the answers and argued accordingly. For long-type questions where the results are not random, the testers check the answers and calculate accordingly. The tests conducted online and passed on to the candidates can be by email or website.

The system can be significantly improved in two main ways. The first place to improve is a teacher labeled question level. The currently proposed system requires the teacher to include a question tag while submitting. In future development, we aim to make this process mechanical which will improve the teaching process. The second area to improve this system is the complete automation of descriptive questionnaires.

6. Limitation

Despite having many advantages and facilities, it has a few potential limitations that we cannot ignore. This system requires permission from the student's camera, microphone, and GYRO to record students' activities from the device they use to attend the exam. It can become an impediment to students' personal inviolable information if the system faces any major breakdown. This system requires a stable internet connection, but most households in Bangladesh have no internet access. The internet outage can become the reason for an imbalance in the learning management system of individual students while attending the exam. The average cost of building the system and maintaining it is a bit high for many institutions and authorities in developing countries like Bangladesh.

7. Conclusion

In the span of the internet metaphors, countries like Bangladesh still facing issues in building a proper e-learning system to handle the covid-19 outburst. This work may help to resolve the critical obstruction of e-learning which is an e-exam. The drawback of the online exams can be overlooked with the help of Artificial Intelligent, Blockchain, RDP, and smart login systems. This paper presents an AI-based blockchain framework that secures the online examination system. It is expected that our proposed system will play a vital role in the evolution of e-learning, where teachers can take a proper exam just like they are physically present in the classroom.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Ehlen G.R. Cluskey Jr, R Craig, Mitchell H. Raiborn, Thwarting online exam cheating without proctor supervision, J. Acad. Bus. Ethics 4. 1 (2011) 1–7.
[2] Kavish Garg, et al., Convolutional neural network-based virtual exam controller, 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), IEEE, 2020.
[3] Mukta Goyal, Divakar Yadav, Alka Choubey, Fuzzy logic approach for adaptive test sheet generation in e-learning, 2012 IEEE International Conference on Technology Enhanced Education (ICTEE), IEEE, 2012.
[4] Im Y. Jung, Heon Y. Yeom, Enhanced security for online exams using group cryptography, IEEE Trans. Educ. 52 (3) (2009) 340–349.
[5] Qingtang Liu, Guilin Fan, Using learning analytics technologies to find learning structures from online examination system, 2014 International Conference Of Educational Innovation Through Technology, IEEE, 2014.
[6] Mojitha Mohandas, et al., Automated question paper generator system, Int. J. Adv. Res. Comput. Commun. Eng. 4 (12) (2015) 676–678.
[7] Dimple V. Paul, et al., Use of an evolutionary approach for question paper template generation, 2012 IEEE Fourth International Conference on Technology for Education, IEEE, 2012.
[8] Chenggang Zhen, Yingmei Su, Research about human face recognition technology, 2009 International Conference on Test and Measurement, IEEE, 2009 Vol. 1.
[9] Apoorv Jain, et al., Smart contract enabled online examination system based in blockchain network, 2021 International Conference on Computer Communication and Informatics (ICCCI), IEEE, 2021.
[10] Kyungmee Lee, Mik Fanguy, Online exam proctoring technologies: educational innovation or deterioration? Br. J. Educ. Technol. (2022).
[11] Qurotul Aini, et al., Digitalization online exam cards in the era of disruption 5.0 using the DevOps Method, J. Educ. Sci. Technol. (EST) 7 (1) (2021) 67–75.
[12] Kenrie Hylton, Yair Levy, Laurie P. Dringus, Utilizing webcam-based proctoring to deter misconduct in online exams, Comput. Educ. 92 (2016) 53–63.
[13] Sanaz Khalili, Ali Shakiba, A face detection method via ensemble of four versions of YOLOs, 2022 International Conference on Machine Vision and Image Processing (MVIP), IEEE, 2022.
[14] CHECKER, Plagiarism, and paraphrasing tool using python, Wesleyan J. Res. 14 (16) (2021) MayISSN–0975-1386.