Design and implementation of secure student score system

Yiming Su

School of Computer Engineering and Science, Shanghai University, Shanghai, 200444, China

symwaley@shu.edu.cn

Abstract. The purpose of designing this system is to provide schools with a new way to make score certifications of a student and a safer way to search for a student's previous academic scores. When a student is applying for a new school to further his study, the school always uses his previous academic scores to decide whether to enroll him. The current way for a school to mark a student and to search for a new student's score record is depend on the student himself, which faces the problem of illegal modification and data leakage. The system mentioned in this paper can add a certification that includes the time information and score information. It can also use the digital signatures of teachers and headmasters to ensure that the scores are given by the corresponding teacher. This system does not include the direct Grade Point Average (GPA), but just includes the raw scores of each subject. Because different schools have different ways to turn the raw scores into a GPA and they also have different GPA upper limitations.

Keywords: student score system, blockchain, asymmetric encryption.

1. Introduction

In high schools, colleges, and universities, teachers use exams to test students' academic performance. So, the scores of the exams have become an intuitionistic standard to evaluate whether a student has good academic attainments [1,2]. When a school is deciding whether to enroll a student, it should check the student's previous score record. It is not hard to understand that schools want to enroll students that are outstanding in academics. And it is also unquestionable that students want to be enrolled in schools that are ranked highly.

However, schools must use the score report which is made by the previous school where the student studied to measure the value of a certain student. But now, most of the universities just publish the picture of their scores report on every student's campus account with just a picture of the stamp belonging to the Office of academic affairs on it. Meanwhile, the transmission and submission of the score report are all done by the student himself. The safety and resistance to modification cannot be guaranteed during the process of transmission. In addition, most universities use different ways to calculate their GPA. Every student gets their raw score after the final examination, and each of the scores they get will be transformed into a float number to intuitively show the total academic performance of this semester. But each school has its algorithm to transform the scores into GPA. Those unimportant courses may have a lower weight while those core courses may have a higher weight. The definite weight and algorithm may be different from school to school. The total amount of GPA is also different among each school, which floats from 4 to 6. There are already a lot of implementations and research on digital signatures and blockchain in the medical area [3,4,5,6], cloud computing [7,8], copy protection [9], and marketing [10,11] to protect users' privacy and money. But there are only a few implementations in the educational field [12]. The current studies in the educational field are focused on the digital diploma, which is the certification of the schooling level of a student. It can be seen that existing works have not covered the security of score certification yet, and the counterfeiting of the score certification has become a serious problem. But the secure score certification system in this paper can reflect the definite academic ability of a student and ensure the safety of the data of each student. This paper uses the digital signature to guarantee the data safety of the score report and to ensure that any illegal modifications can be recognized by verifying the signature directly. And this paper uses blockchain to store and hash the score and signature information, it can implement the addition, modification, and research of the stored score certification. The signing, verifying, updating, and researching of the system are covered in Section 2 along with some fundamental information on the RSA signing technique, which will be employed as the primary signing algorithm in our system. In section 2, the framework will be displayed. The most recent efforts, which include system implementation specifics, are displayed in Section 3 of the document. Different users can use different functions to ensure the feasibility of the system. Section 4 shows the conclusion, disadvantages, and future expectations of related works.

2. The secure student score system

2.1. Overview of secure student score system

To guarantee the security of the E-score system, three main requirements must be satisfied. First is the authentication, which means the identity of the person who signed for the score certification can be recognized by verifying the signature. Second is the completeness, which means the score cannot be modified after signing for it, in other words, any modifications added to the score after is signed can be recognized by verifying the signature. Third is non-repudiation, which means the person who signed for the score cannot claim that he did not sign for it. To achieve these three goals, the E-score system includes the following four functions: signing, modifying (only by the teacher who signed for the score), searching, and submitting. The system allows teachers to sign for the score that was worked out from the test paper of the examination. Each teacher has his private key and public key. The public key should be announced to enable others to verify the signature, and the private key is used for signing for the score and should be kept properly by the teacher himself. The score list of each student can be considered as a block, after writing the subject and the corresponding score on it, the teacher can sign for his subject. After all the subjects and the corresponding scores are written and signed, the new block is completed and can be sent to the headmaster. The job of the headmaster is to verify whether each signature and score are corresponded. If the block is considered valid and signed by the headmaster using his private key, it will be sent to the Ministry of Education. After the final verification and signing by the Ministry of Education, the score certification will be considered valid by the law and it will become the next chain of the blockchain which was stored by the school and the Ministry of Education. Figure 1 depicts the system's high-level architecture.

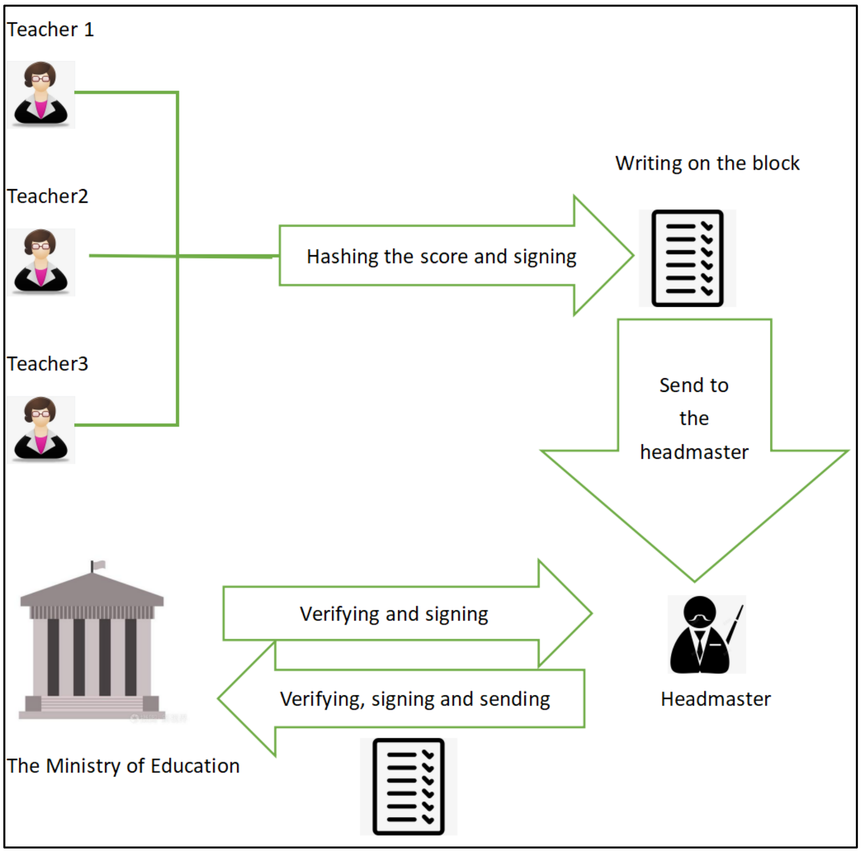


Figure 1. The framework of the system.

2.2. *Detail of design*

2.2.1. The RSA algorithm. The system uses the RSA algorithm for signing the score. The RSA algorithm is raised by Ron Rivest, Adi Shamir, and Leonard Adleman in 1977. It is a public key cryptographic algorithm [13], which means it has two different keys, the private key, and the public key. The public key is known to all to verify the legality of the signature. And the private key is kept only by the owner of the key. There are three major steps in the RSA algorithm, key generation, encryption, and decryption [14,15].

2.2.2. Generating the score certification. The teachers first generate their own private keys and public keys, which are two prime numbers that have the same length. Their private keys are handed in and kept in the server run by the school. Figure 2 shows this process. The headmaster of each school also needs to generate his private key and public key, which represents the school. The length of the keys of the headmaster should be longer than the teachers' keys. Because the headmaster's signature secures all the scores are correct. In RSA encryption, the longer key has higher security. The headmasters' public keys are submitted to the Ministry of Education, which means each school has a public key to verify the score list they send to the government. The headmasters' signatures represent their schools.

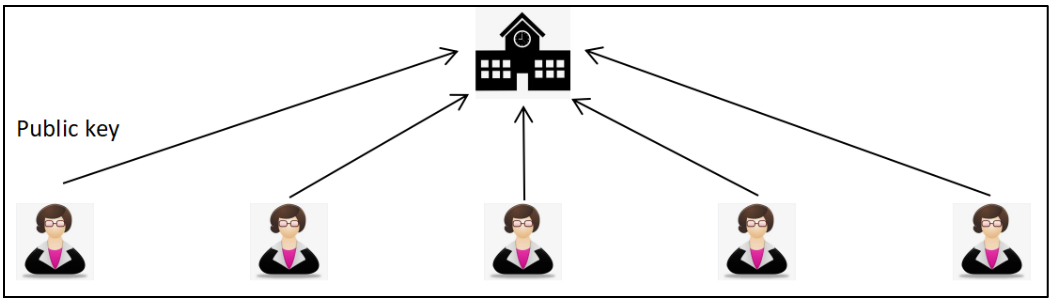


Figure 2. The transmission of teachers' public keys.

When the teacher works out a student's score, he can write his subject and the corresponding score on the score report. Then he should sign for what he wrote just like what Figure 3 shows. He first adds the time of signing to the subject and score, then compute the hash value of this information [16]. Then he just signs for the information by encrypting the hash value he has just worked out. The encryption process uses the private key which is kept only by the teacher. The whole encryption process can be done by using Xilinx 14.2 tool [17].

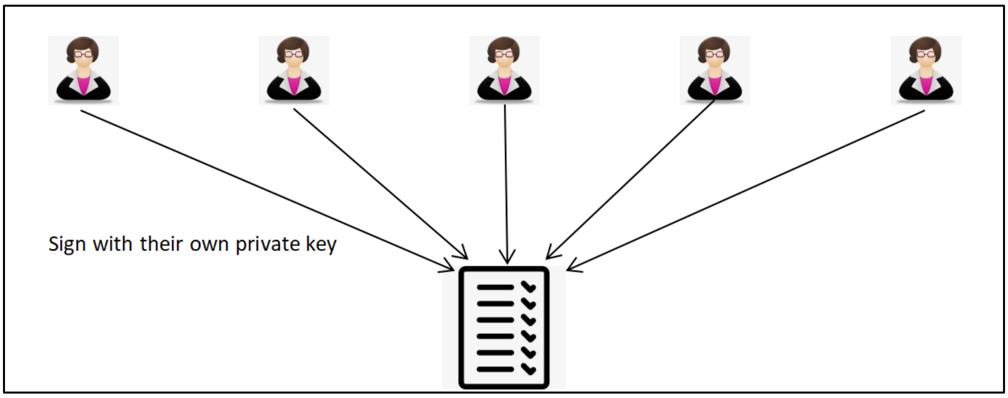


Figure 3. The signing of the teachers.

After all the teachers finish writing and signing the score report, it will be sent to the headmaster of the school. The job of the headmaster is to verify if all the signatures can perfectly match the scores and subjects. The teachers' public keys were stored in the server of the school. The headmaster uses the public key to decrypt the signature and get the hash value A. He then computes the true hash value B of the score information. If A is as same as B, the signature and information are considered valid.

After all the signatures and scores are proven to be valid, the headmaster should use his private key to sign for it as Figure 4, which means the school approves of this score report. The signing process is the same as what the teachers did. He should add the time of signing to the raw information and getting the hashing value [16], then use his private key to encrypt the hash value and add the ciphertext after the raw information. Then it will be sent to the Ministry of Education which is set up by the government to have the final verification. The headmasters' public keys are sent to the government as Figure 5.

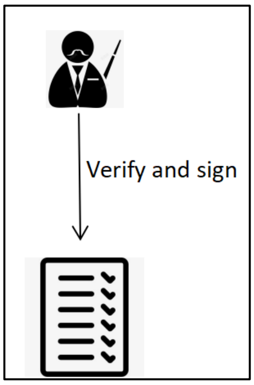


Figure 4. The signing of the headmaster.

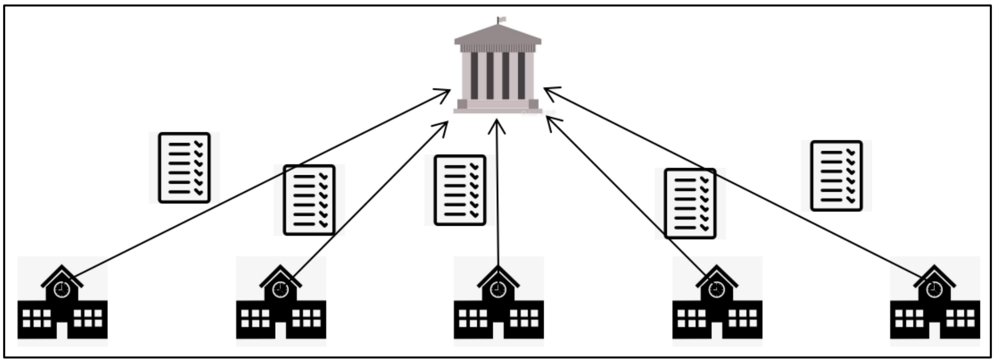


Figure 5. The transmission of score certifications signed by schools.

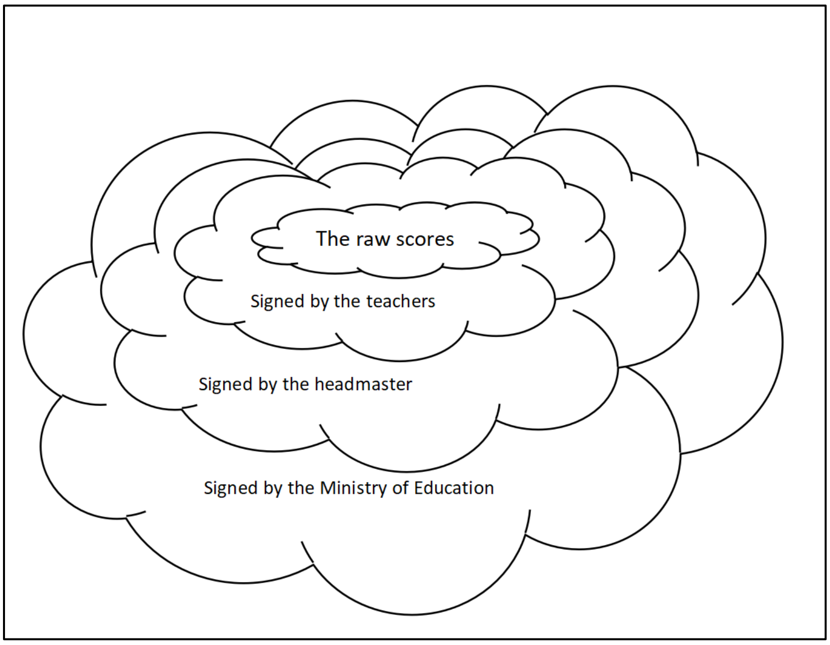


Figure 6. The relationship between all the signatures.

The job of the Ministry of Education is to check if the signature of the school is valid, and was signed by the headmaster of the school. The public key of each school is stored by the government. The government men just do the same job as the headmasters did, which is verifying the signature by the public key. If the score report is exactly from the school, the government will use its private key to sign for it to guarantee its validity of it. Figure 6 shows the relationship between all the signatures.

If the score report is committed by the government, it will have the force of law which can be used to certify the student's academic performance. Once the verification of the score report is done by the government, it will be sent back to the school and become the next chain of the blockchain which is stored by the school. Figure 7 shows the process of the verification of the score.

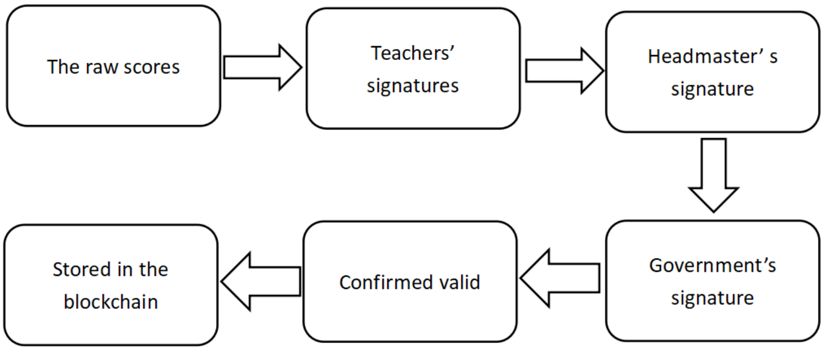


Figure 7. The running process of the system.

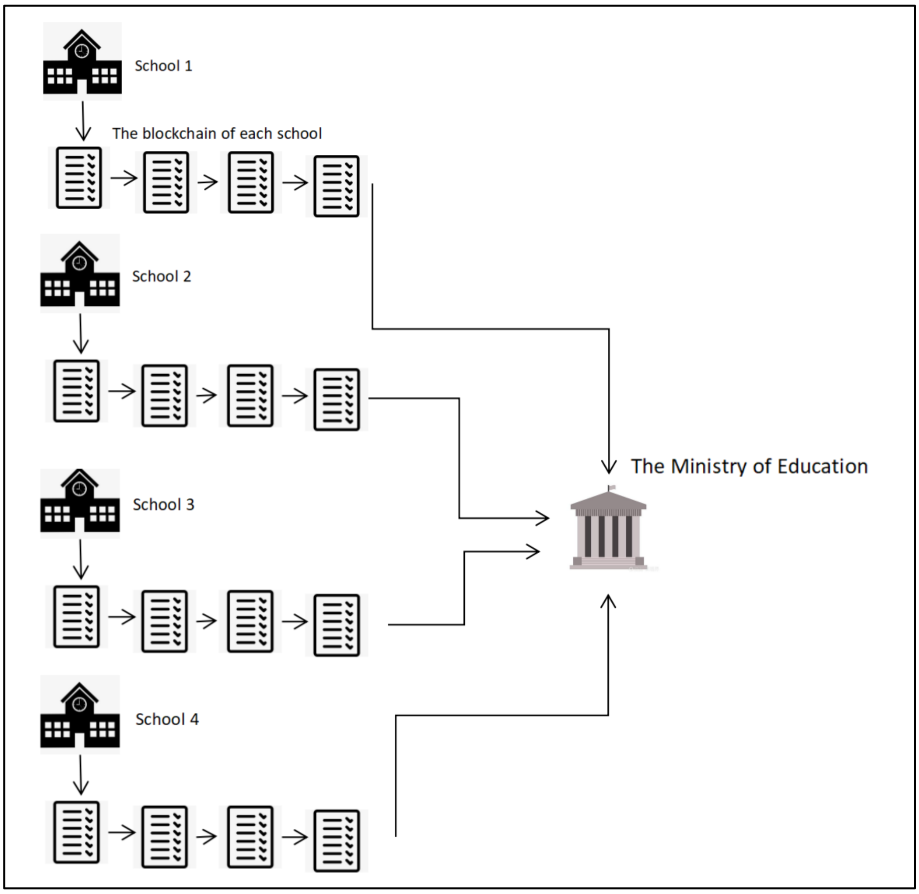


Figure 8. The storage relationship between schools and the Ministry of Education.

Every school only stores the certification of its student, and the Ministry of Education set by the government stores all the students' certifications of each school, which is called the main chain. In other words, each school has a copy of a part of the main chain, which includes each student who is currently studying in the school. Figure 8 shows the storage relationship between schools and the Ministry of Education.

2.2.3. Application of the secure student score system. When a student is applying for a different school from which he is already in, the school can search the database of the Ministry of Education for the student's certification of scores. If the school wants to enroll the student, the school can add the certification to the blockchain and let it be the next chain. The new school can record his scores just after the existing record which was written by the last school. The new record is only stored by the new school and the government. Figure 9 shows the brief process of applying and searching.

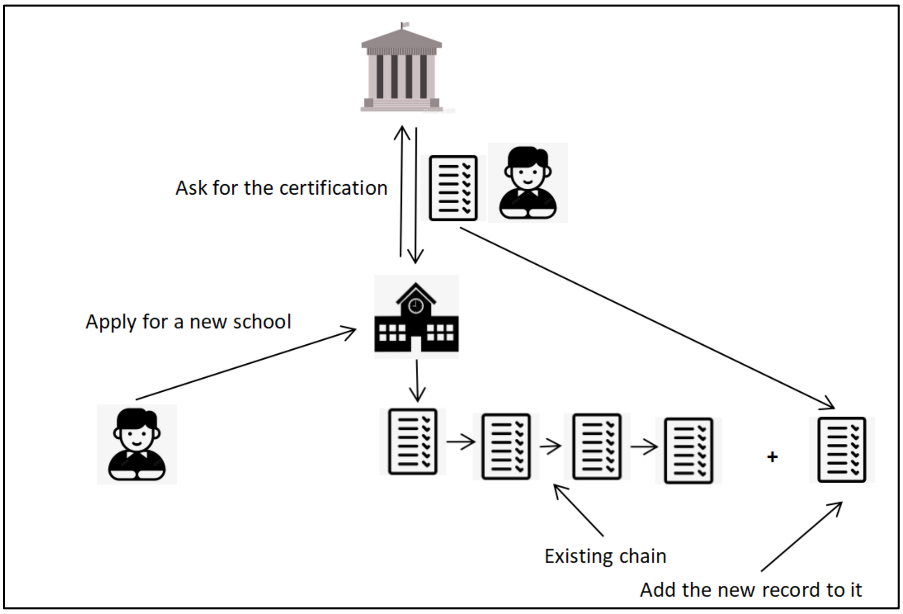


Figure 9. The process of applying and searching.

2.2.4. Modification of the current recordings. If the school wants to modify the existing record which is already stored by the Ministry of Education and another school, it can just do the modification to the chain of that student on the school's blockchain and notify the Ministry of Education to modify on its main blockchain. After the modification of the main chain, other schools will check if it stores that student's certification and modify it as well.

The process of modification is as same as the process of verifying as Figure 10 shows. The teacher needs to delete the invalid information and add new information to it. Then does the same thing as generating the score certification.

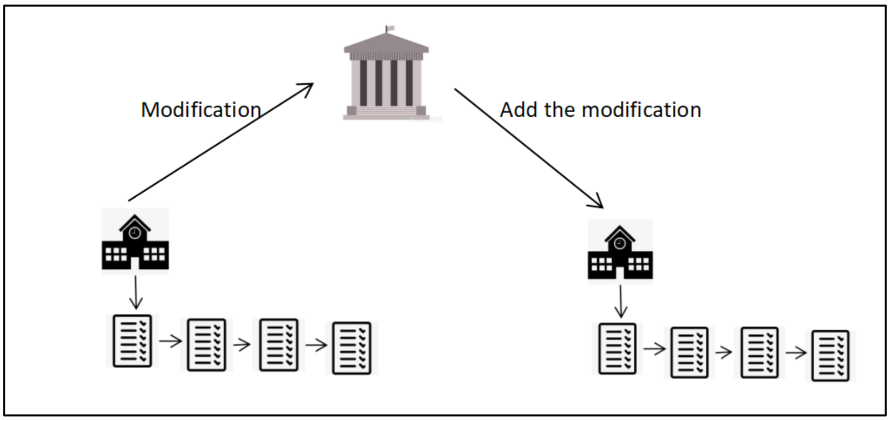


Figure 10. The process of modifying the current certification.

2.2.5. The graph of score certification. If the picture of the certification is needed, the signature can be adjusted into the digital watermark by using the CS-SC-DWT-SVD-based image watermarking scheme [18] and implanted into the picture of the score certification. It is certainly not easy to be modified illegally [19].

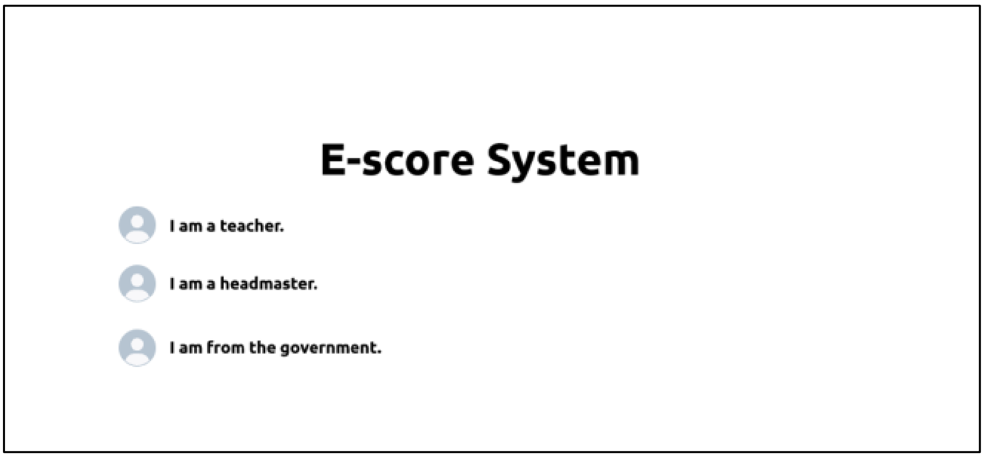
3. Implementation of the system

This section will show a brief demonstration of the specific implementation of the Secure Student Score System, which includes the functions provided to the different users.

3.1. Users' function designing

The following part shows the function used by teachers, headmasters, and the government. The definite steps for realizing these functions will also be shown.

3.1.1. The interface



E-score System

I am a teacher.

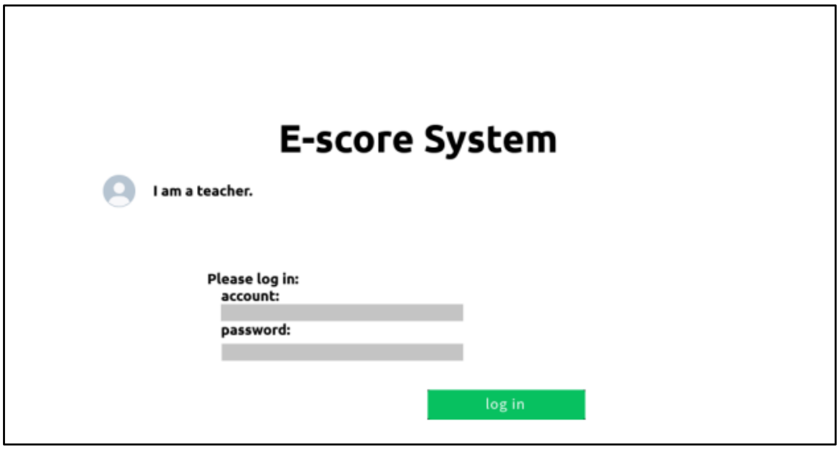
I am a headmaster.

I am from the government.

Figure 11. The choosing interface of the system.

The system faces three kinds of users: teachers, headmasters, and government users. The person who wants to use the system should choose their identity first just as Figure 11 shows.

3.1.2. The teachers' side

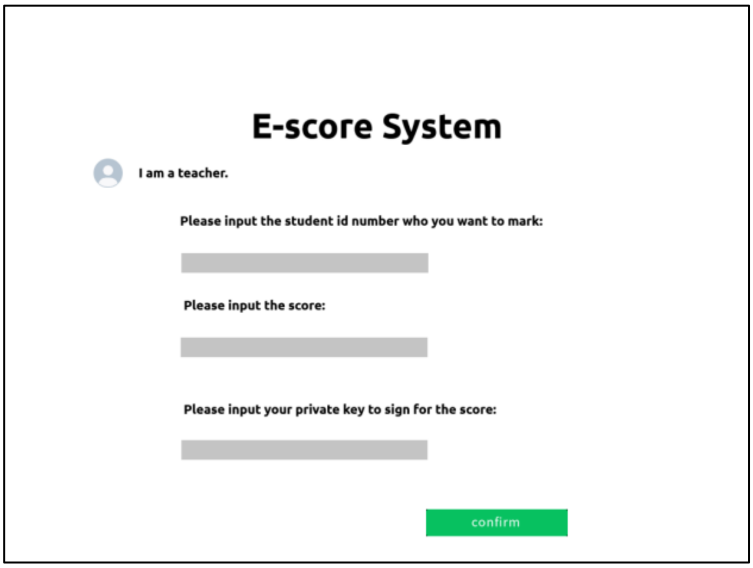


E-score System

I am a teacher.

Please log in:
account:
password:

Figure 12. The login entrance of teachers.



E-score System

I am a teacher.

Please input the student id number who you want to mark:

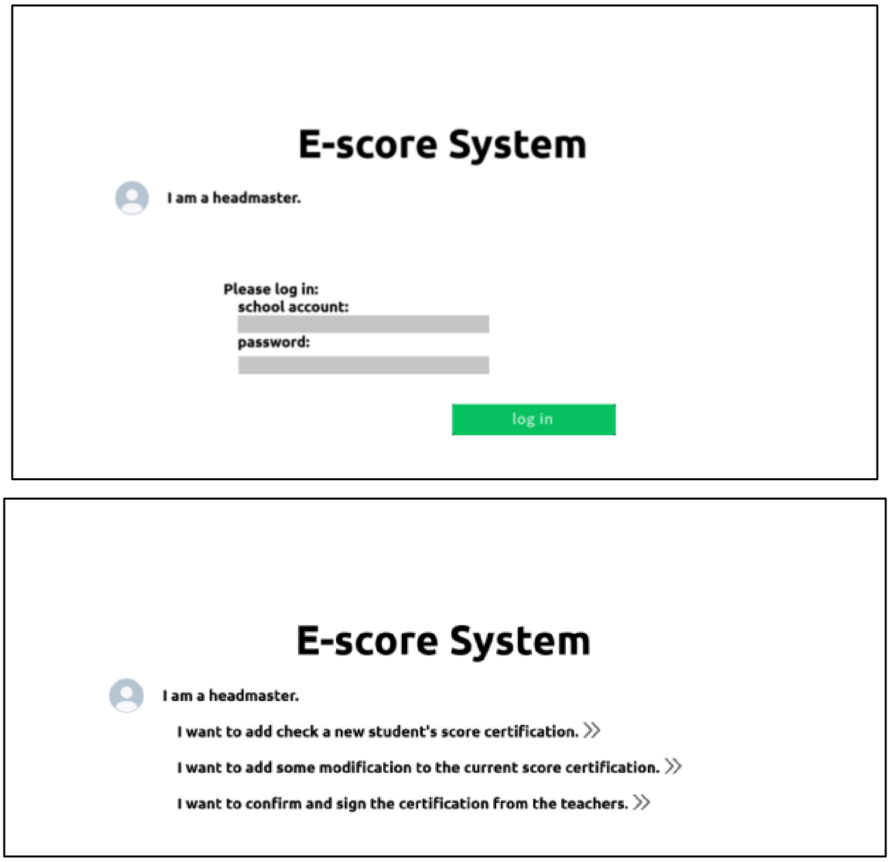
Please input the score:

Please input your private key to sign for the score:

Figure 13. The signing of teachers.

Each teacher has his account. The subject he teaches and his personal information are included in the account information. This information and login system is contributed by and stored by the school. Teachers can log in and sign like what Figure 12 and Figure 13 show.

3.1.3. The headmaster's side



E-score System

I am a headmaster.

Please log in:
school account:
password:

E-score System

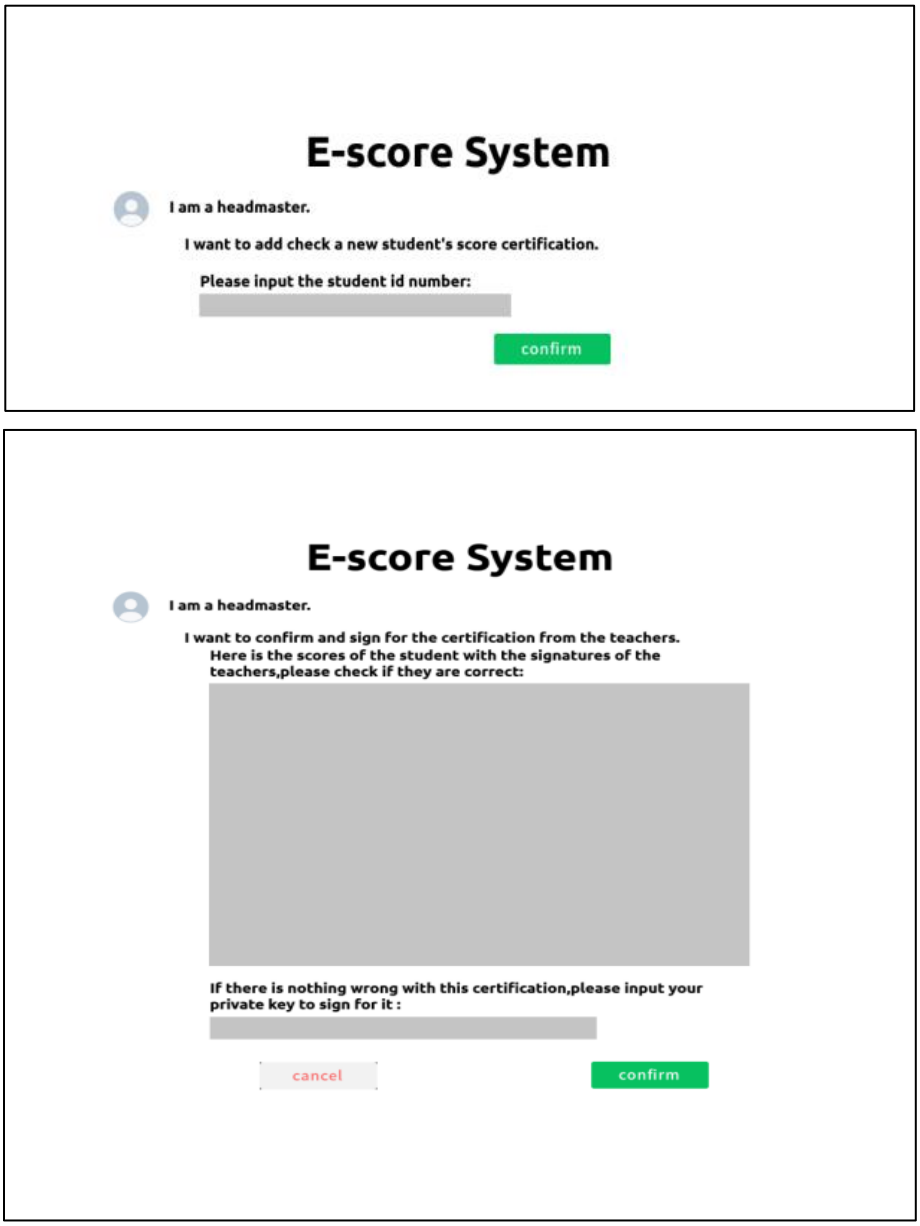
I am a headmaster.

I want to add check a new student's score certification. »

I want to add some modification to the current score certification. »

I want to confirm and sign the certification from the teachers. »

Figure 14. The login entrance and functions for headmasters.



E-score System

I am a headmaster.

I want to add check a new student's score certification.

Please input the student id number:

E-score System

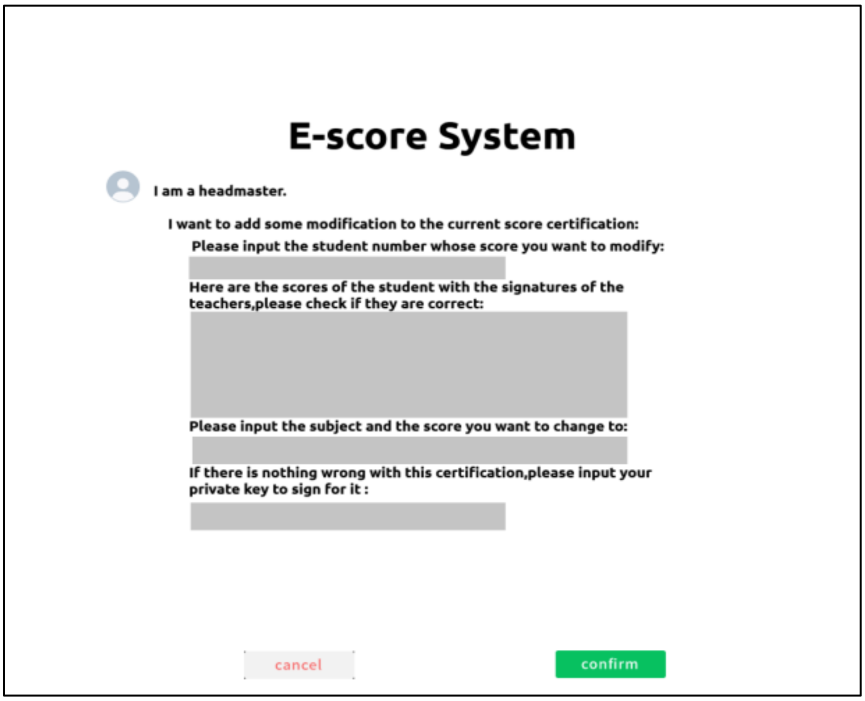
I am a headmaster.

I want to confirm and sign for the certification from the teachers.

Here is the scores of the student with the signatures of the teachers,please check if they are correct:

If there is nothing wrong with this certification,please input your private key to sign for it :

Figure 15. The interface of searching for a new student and signing.



E-score System

I am a headmaster.

I want to add some modification to the current score certification:

Please input the student number whose score you want to modify:

Here are the scores of the student with the signatures of the teachers,please check if they are correct:

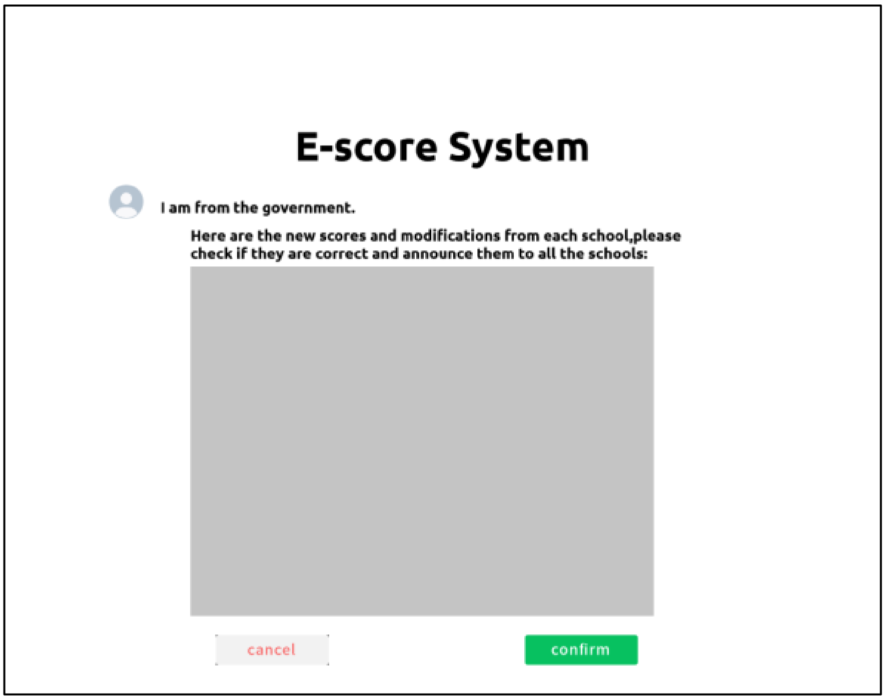
Please input the subject and the score you want to change to:

If there is nothing wrong with this certification,please input your private key to sign for it :

Figure 16. The modification by headmasters.

The headmasters have the power to represent the school. The information on school accounts is stored by the government. The headmaster can use the system to modify and check the report handed in by teachers and ask the government for a new student's score certification. Figure 14, Figure 15, and Figure 16 show the functions provided to the headmasters.

3.1.4. The government's side



E-score System

I am from the government.

Here are the new scores and modifications from each school,please check if they are correct and announce them to all the schools:

Figure 17. The signing of government users.

The government is the leader of this system and can finally verify if the score certification is valid just as in Figure 17.

3.2. Algorithm of secure score certification

The algorithm means that the input of the hash function includes the subject, the score information, the timestamp provided by the operating system, and the block number. The process of adding a new block to the blockchain is to link the block to the last block of the chain.

Algorithm 1. Hashing and addition of the blocks

```
Input: subject, score, timestamp, and student number
Output: the hash value and the next block
for i=0 to blockNum -1 do
    h ← subject + score + timestamp + student number
    h ← sha256 (h) // Sha256 is a hashing function to compute the unique hash function.
    h ← hexdigest (h) // This function is used to turn the binary data into hexadecimal data.
    previous block’s next block ← blockNum
    next block ← 0
end for
```

3.3. Security analysis

The security of the RSA algorithm has been proved by mathematicians. The safety of the RSA encrypting algorithm is based on decomposing prime factors of large numbers, and this problem can not be solved within reasonable time limitations until now. In other words, a fast way to decompose prime factors of large numbers does not exist. The only way to solve the problem is to use the computers to enumerate the number with its hash power.

However, many attacking protocols aiming at RSA encrypting algorithms have been raised. Such as mathematical attacks aiming at the decryption key [20], attacks on small-exponent RSA problems using Coppersmith's method [21], cache-based side-channel attacks [22], or using the bit-stuffing technique [23]. The safety of the common RSA signing algorithm has been threatened enormously and attackers can sometimes decrypt the RSA signatures if the public keys and private keys are not long or flexible enough. But new signing models have been raised at the same time. For example, scientists have made a lot of progress in the field of quantum computers, so using the quantitating keys to sign for the files can effectively avoid the known plaintext attack [24]. When applying the system to real use cases, this paper can use the ESRKGS to consider security and usability. Its security has been enhanced compared to the conventional RSA algorithm [25]. The time for it to against the Brute-force attack time is largely longer than RSA1 and RSA2 algorithms.

3.4. Details of technology of blockchain

3.4.1. Hash algorithm. Hash functions, also known as hash values or message digests, are irreversible one-way maps that may convert an input message M of any length into a brief, fixed-length hash H(M). Another thing to keep in mind is that this is a one-way cryptosystem, meaning there is only encryption and no decryption, making it challenging to reverse the process. Hashing algorithms can be used on both messages and pictures [26]. But there is still a little possibility that the collision may affect the hash algorithm. So, this paper can use new technology and enhanced hash functions with a stronger ability to avoid collision resistance such as chameleon hash [27] to work out the hash value of a message. As IPV6 is dominating the Internet, there are also hash functions for IPv6 network data [28].

3.4.2. Distributed storage. A method of leveraging disk space on various computers over a network to create a virtual storage device out of these dispersed storage resources is known as distributed storage. In the implementation of our Secure Student Score System, each student’s score certification is stored separately by each school’s server. The school server may not have too much storage capacity. And the government stores the certifications of all the students as backups to avoid data corruption in schools. Each school is distributed system that can use clustering technology to lower the cost of storage space and energy [29].

4. Conclusion

The present research shows the framework and details of the implementation of the secure student score certification system. It provides a newer and safer way for schools and teachers to manage students' scores and academic levels. It also can avoid illegal modifications, which means modifications add by those who do not have the right to sign can be recognized at once. However, there are still a lot of disadvantages to the systems. For example, the safety of using the RSA algorithm has not been testified and the signing speed has not been compared by using different signing algorithms. These works can be done in the future studies.

References

[1] Anna M. Biller, Karin Meissner, Eva C. Winnebeck and Giulia Zerbini 2022 *Sleep Medicine Reviews* School start times and academic achievement - A systematic review on grades and test scores vol 61 p 101582.

[2] J.D. Allen 2005 The Clearing House Grades as valid measures of academic achievement of classroom learning vol 78 pp 218-223.

[3] Nagasubramanian, G., Sakthivel, R.K., Patan and R. et al. 2020 *Neural Comput & Applic* Securing e-health records using keyless signature infrastructure blockchain technology in the cloud vol 32 pp 639–647

[4] Pranav Ratta, Amanpreet Kaur, Sparsh Sharma, Mohammad Shabaz, and Gaurav Dhiman 2021 *Journal of Food Quality* Application of Blockchain and Internet of Things in Healthcare and Medical Sector: Applications, Challenges, and Future Perspectives vol 2021

[5] Jafar A. Alzubi 2021 *Computer Communications* Blockchain-based Lamport Merkle Digital Signature: Authentication tool in IoT healthcare vol 170 pp 200-208

[6] Anushree Tandon, Amandeep Dhir, A.K.M. Najmul Islam and Matti Mäntymäki 2020 *Computers in Industry* Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda vol 122 p 103290

[7] Yuan Xue, Yu-an Tan, Chen Liang, Yuanzhang Li, Jun Zheng, and Quanxin Zhang 2018 *Information Sciences* RootAgency: A digital signature-based root privilege management agency for cloud terminal devices vol 444 pp 36-50

[8] U.Somani, K. Lakhani and M. Mundra 2010 *2010 First International Conference On Parallel, Distributed and Grid Computing (PDGC 2010)* Implementing digital signature with RSA encryption algorithm to enhance the Data Security of cloud in Cloud Computing pp 211-216

[9] Edlira Martiri and Artur Baxhaku 2012 *Procedia Technology* Monotone digital signatures: an application in software copy protection vol 1 pp 275-279

[10] Alex Marthews, Catherine Tucker 2023 *International Journal of Research in Marketing* What blockchain can and can't do: Applications to marketing and privacy vol 40 pp 49-53

[11] Abhinav Pal, Chandan Kumar Tiwari and Nivedita Haldar 2021 *The Journal of High Technology Management Research* Blockchain for business management: Applications, challenges and potentials vol 32 p 100414

[12] A Finandhita and I Afrianto 2018 IOP Conf. Ser.: Mater. Sci. Eng. Vol 407 p 012109

[13] Shieh, Ming Der, Jun-Hong Chen, Hao-Hsuan Wu, and wen-Ching Lin. 2008 *IEEE Transactions on Very Large-Scale Integration (VLSI) Systems* A New Modular Exponentiation Architecture for Efficient Design of RSA Cryptosystem vol 16 pp 1151-1161

[14] Rahman, Mostafizur, Iqbalur Rahman Rokon, and Miftahur Rahman. 2009 *2009 3rd International Conference on Anti-counterfeiting, Security, and Identification in Communication* Efficient hardware implementation of RSA cryptography pp 316-319

[15] Sheba Diamond Thabah, Mridupawan Sonowal, Rekib Uddin Ahmed and Prabir Saha 2019

Procedia Computer Science Fast and Area Efficient Implementation of RSA Algorithm vol 165 pp 525-531

[16] Aleksandra V. Tutueva, Artur I. Karimov, Lazaros Moysis, Christos Volos and Denis N. Butusov 2020 *Chaos, Solitons & Fractals* Construction of one-way hash functions with increased key space using adaptive chaotic maps vol 141 p 110344

[17] Sheba Diamond Thabah, Mridupawan Sonowal, Rekib Uddin Ahmed and Prabir Saha 2019 *Procedia Computer Science* Fast and Area Efficient Implementation of RSA Algorithm vol 165 pp 525-531

[18] Anirban Bose, Santi P. Maity 2022 *Journal of Information Security and Applications* Secure sparse watermarking on DWT-SVD for digital images vol 68 p103255

[19] Taybeh Salehnia, Abdolhossein Fathi 2021 *Expert Systems with Applications* Fault tolerance in LWT-SVD based image watermarking systems using three module redundancy technique vol 179 p 115058

[20] Willy Susilo, Joseph Tonien 2021 *Theoretical Computer Science* A Wiener-type attack on an RSA-like cryptosystem constructed from cubic Pell equations vol 885 pp 125-130

[21] Stephen D. Miller, Bhargav Narayanan and Ramarathnam Venkatesan 2021 *Journal of Number Theory* Coppersmith's lattices and “focus groups”: An attack on small-exponent RSA vol 222 pp 376-392

[22] Maria Mushtaq, Muhammad Asim Mukhtar, Vianney Lapotre, Muhammad Khurram Bhatti and Guy Gogniat 2020 *Information Systems* Winter is here! A decade of cache-based side-channel attacks, detection & mitigation for RSA vol 92 p 101524

[23] Falowo O. Mojisola, Sanjay Misra, C. Falayi Febisola, Olusola Abayomi-Alli and Gokhan Sengul 2022 *Egyptian Informatics Journal* An improved random bit-stuffing technique with a modified RSA algorithm for resisting attacks in information security (RBMRSA) vol 23 pp 291-301

[24] Wenxue Tan, Xiping Wang, Xiaoping Lou, Meisen Pan 2011 *Procedia Engineering* Analysis of RSA based on Quantitating Key Security Strength vol 15 pp 1340-1344

[25] M. Thangavel, P. Varalakshmi, Mukund Murrali and K. Nithya 2015 *Journal of Information Security and Applications* an Enhanced and Secured RSA Key Generation Scheme (ESRKGS) vol 20 pp 3-10

[26] Sean McKeown, William J. Buchanan 2023 *Forensic Science International: Digital Investigation* Hamming distributions of popular perceptual hashing techniques vol 44 p 301509

[27] Chunhui Wu, Lishan Ke, Yusong Du 2021 *Information Sciences* Quantum resistant key-exposure free chameleon hash and applications in redactable blockchain, vol 548 pp 438-449

[28] Ying Hu, Guang Cheng, Yongning Tang, Feng Wang 2020 *Computer Communications* A practical design of hash functions for IPv6 using multi-objective genetic programming, vol 162 pp 160-168

[29] Paul W. Poteete, 2023 *Array* Organically distributed sustainable storage clusters vol 17 p 100275