International Journal of Engineering Science and Advanced Technology (IJESAT)

IJESAT (Enriching the Research)

Open Access Research Article

Volume: 23 Issue: 07

July, 2023

CERTIFICATE VALIDATION WITH SHA

Mrs. L.L. Sai Maneesha [1], R. G V D Nagesh [2], N. Ganga Mahalakshmi [3], V. Swetha Yamini [4], M. Srinivas [5]

[1] Assistant Professor, Department of CSE, Ramachandra College of Engineering, Eluru, A.P

[2,3,4,5] UG Students, Department of CSE, Ramachandra College of Engineering, Eluru, A.P

ABSTRACT

Lakhs of people getting Degree's year after year, due to the lack of effective anti-forge mechanism, events that cause the graduation certificate to be forged often get noticed. In order to solve the problem of counterfeiting certificates, the digital certificate system based on SHA and Digital signature technology. All the illegal activities filled against a person and all the activities are updated in the Personal ID. Using the modification process we would monitor the degree certificate. We deploy Unique based monitoring using this system. The main aim of this project is to secure academic certificate and for accurate management and to avoid forge certificate. To achieve all this features, we are converting all certificates into digital signatures and this digital signature will be stored in local server the digital signature is retrieve from the file at the time we need to verify. The same data is stored in different blocks to perform security feature. If by any chance if its data got altered then verification gets failed at next block storage and user may get intimation about data altered. Here in this project, we need provide two views for students and institutes bot the view are separate we will provide first they need to login and they can valid the certificates the software technology we are used in this project to develop the frontend we use the python Tkinter library. Middleware python we used to develop and the details are stored in the local server file. The user first register with mail id and he will direct to the login entering the password he can perform the internal operations. The original certificate has particular has value when user need validation his certificates, he needs to upload his certificate the digital signature will check whether certificate is original or not.

1. INTRODUCTION

Now a days the world is developing fast the internet use age is high as we compare to olden days. Our project is certificate validation with SHA in this the user can validate the certificate is original or not. He checks with the help of Digital signature with is produced to the certificate. Now days the companies are verify the certificate through online it may chance to get fraud the certificate. To avoid the certificate fraud, we need to develop this certificate validation with SHA. Here in this first the has value and the digital certificate was generated to the certificate with user details. The hash value and the digital signature was stored in the text file of local server. At the time of validation of certificate, the system will take the hash value and the digital signature is taken from the text file which is already there. And for uploaded file the hash code is generate then it compares the both digital signatures. The

IJESAT (Enriching the Research)
Open Access Research Article
Volume: 23 Issue: 07
July, 2023

system says that whether the certificate is original or not. In this way it will check to develop this we used some algorithms they are SHA256(secure hashing algorithm) and Digital signature with help of this we perform the operation. Certificate validation is a crucial part of digital security, and it is essential to ensure that the certificate presented is genuine and has not been tampered with. In this project, we will discuss certificate validation using SHA and digital signatures. We will explore the concepts of SHA and digital signatures and how they are used to ensure the authenticity of certificates.

SHA (Secure Hash Algorithm):

SHA is a cryptographic hash function that generates a fixed-length output from an input of variable length. The output, known as a hash value, is unique to the input, and even a slight change in the input results in a completely different hash value. The SHA algorithm was developed by the National Security Agency (NSA) and is widely used in digital security. SHA-1 was the first version of the SHA algorithm, but it has been deprecated due to security concerns. SHA-2 is the current version of the SHA algorithm and is considered more secure than SHA-1. SHA-2 has several variants, including SHA-256, SHA-384, and SHA-512. SHA-0: A retronym applied to the original version of the 160-bit hash function published in 1993 under the name "SHA". It was withdrawn shortly after publication due to an undisclosed "significant flaw" and replaced by the slightly revised version SHA-1. SHA-1: A 160-bit hash function which resembles the earlier MD5 algorithm. This was designed by the National Security Agency (NSA) to be part of the Digital Signature Algorithm. Cryptographic weaknesses were discovered in SHA-1, and the standard was no longer approved for most cryptographic uses after 2010. SHA-2: A family of two similar hash functions, with different block sizes, known as SHA-256 and SHA-512. They differ in the word size; SHA-256 uses 32-bit words where SHA-512 uses 64-bit words. There are also truncated versions of each standard, known as SHA-224, SHA- 384, SHA-512/224 and SHA-512/256. These were also designed by the NSA. SHA-3: A hash function formerly called Keccak, chosen in 2012 after a public competition among non-NSA designers. It supports the same hash lengths as SHA-2, and its internal structure differs significantly from the rest of the SHA family. Digital Signature: A digital signature is a mathematical technique used to verify the authenticity of digital messages or documents. It uses a public key infrastructure (PKI) to generate a unique digital signature, which is appended to the document. The digital signature can then be verified using the public key of the sender. To create a digital signature, the sender first generates a hash of the document using a cryptographic hash function such as SHA-2. The sender then encrypts the hash using their private key, creating the digital signature. The recipient can then use the sender's public key to decrypt the signature and verify the document's authenticity. The newest specification is: FIPS 186-4 from July 2013. DSA is patented but NIST has made this patent available worldwide royalty-free. A draft version of the specification FIPS 186- 5 indicates DSA will no longer be approved for digital signature generation, but may be used to verify signatures generated prior to the implementation date of that standard.Certificate Validation: Certificate validation is the process of verifying the authenticity of a certificate presented by a website or device. The certificate contains information about the website or device, including the name, public key, and expiration date. Certificate validation is essential to ensure that the certificate is genuine and has not been tampered with. When a user visits a

IJESAT (Enriching the Research)
Open Access Research Article
Volume: 23 Issue: 07
July, 2023

website with an SSL/TLS certificate, the browser checks the certificate's validity. The browser first checks whether the certificate is signed by a trusted certificate authority (CA). If the certificate is signed by a trusted CA, the browser then checks whether the certificate has expired or has been revoked. To check whether the certificate is signed by a trusted CA, the browser uses the CA's public key to verify the digital signature on the certificate. The digital signature is created using the CA's private key and the SHA-2 hash function. The browser then checks whether the certificate has expired or has been revoked by checking the certificate's validity period and the certificate

revocation list (CRL).

In this project to secure academic certificate and for accurate management and to avoid forge certificate we are converting all certificates into digital signatures and this digital signature will be stored in local server as this tamper proof data storage and alter its data and if by an chance if its data alter then verification get failed at next block storage and user may get intimation about data alter.
In SHA technology same transaction data stored at multiple servers with hash code verification and if data alter at one server, then it will be detected from other server as for same data hash code will get different.
In each data will be stored by verifying old hash codes and if old hash codes remain unchanged then data will be considering as original and unchanged and then new transaction data will be appended to local server file as new block. For each new data storage all blocks hash code will be verified.
In this project we have designed following modules

Save Certificate with Digital Signature: Using this module admin user can upload student details and student academic certificate and then application convert certificate into digital signature and then signature and other student details will be saved in local server in file format.
Verify Certificate: In this module verifier or companies or admin will take certificate from student and then upload to application and then application will convert certificate into digital signature and this digital signature will get checked/verified at local server and if matched found then it will retrieve all student details and display to verifier and if match not found then this certificate will be considered as fake or forge.

2. LITERATURE SURVEY

Universities issue certificates to students who have completed the graduation. A graduation certificate is mostly in the form of a paper-based document, an electronic document cannot effectively replace a physical certificate . However, due to the presence of advanced and cheap scanning and printing technologies, the forgery of certificates has increased. This threatens the integrity of the certificate holder and the university that issued the certificate . It is necessary to validate that the graduation certificate presented by the graduate is genuine and the holder is the rightful owner[5]. Moreover, a graduation certificate has to be verified to ensure that its content is correct and also to ensure that the certificate comes from an authentic source. To check the validity, much time will be spent in either reaching out to the university to verify a certificate or in awaiting a reply from the university to confirm that the certificate is valid, and the information is accurate. This process can be extremely laborious and

IJESAT (Enriching the Research)
Open Access Research Article
Volume: 23 Issue: 07
July, 2023

expensive. Making certificates easily verifiable is one advantage of digital systems. In our project , we have decided to explore the field of blockchain to implement our solution. The platform used for implementation is Hyperledger.

3. EXISTING SYSTEM

- The existing system is two types one is physical checking of the certificate and another is online verification.
- Physical checking verification the certificate is check by humans with their hands fir example the certificate is send to the college or any other organization they will check the certificate with hands whether the certificate is original or not.
- The certificate is stored in centralized manner and verified manually, so it takes too much time to verify. There is no safety to the certificate that is given to any private sector.
- Online verification: In this they validate the certificate with the help of any applications are they will check the certificate.
- There are some applications in online they are.

Document verification:

- In this application you can upload the certificate and verification.

Certificate validation: -

- This Application is used to verify the correctness of the Certificate produced by Candidate. This application is useful at the time of Interview in Government Department

DISADVANTAGES OF EXISTING SYSTEM:

- Time consuming Error prone
- Large volume of data
- The user interface is not so good in some applications Only some certificates can be verified.

4. PROPOSED SYSTEM

In our proposed system we need provide the admin view and user view separately because to improve the security and not get the certificate fraud. The admin can create the digital signature for the certificate and this digital signature and hash value was stored in the local server file. The user can check or validate the certificate is original or not. For example, here one college or university will give the certificate to the student if they hardcopy they may can create another duplicate certificate or he they can forgery the certificate. If they give digital certificate to the student then there is less chance to get forgery. In this case the university should first create the digital signature to the certificate with the student details. And digital signature of the certificate should store in the file. In case of any companies

IJESAT (Enriching the Research)
Open Access Research Article
Volume: 23 Issue: 07
July, 2023

ask the certificate verification of the student, in this case the student will submit his digital certificate to that company.

To validate the certificates the college or university gives the digital signature to the company they can easily validate the user certificate through our system. The companies may easily now weather the certificate are original or not. And the certificates are belonged to that student or not they can easily now. The digital signature makes the work simple and easy.

ADVANTAGES OF PROPOSED SYSTEM

- The user view is simple.
- The organization only creates the digital signature to certificate.
- The user can easily validate the certificate.
- Reduce the time by avoiding manual validating the certificate.
- Eliminates manual intervention as far as possible

Error free modification facilities

ISSN No: 2250-3676

IJESAT
(Enriching the Research)

Open Access Research Article
Volume: 23 Issue: 07
July, 2023

5. RESULTS

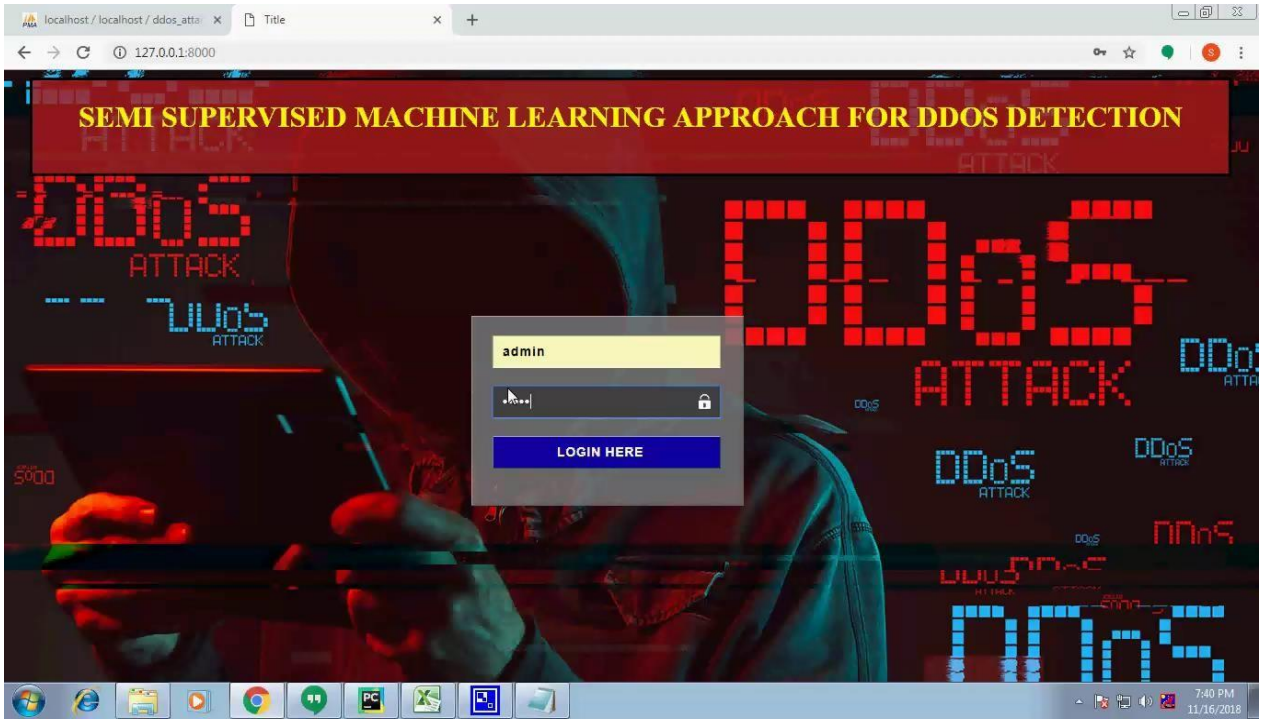

Fig:1 RGISTRATION PAGE

Fig:2 LOGIN PAGE SCREEN SHOT

IJESAT
(Enriching the Research)

Open Access Research Article
Volume: 23 Issue: 07
July, 2023

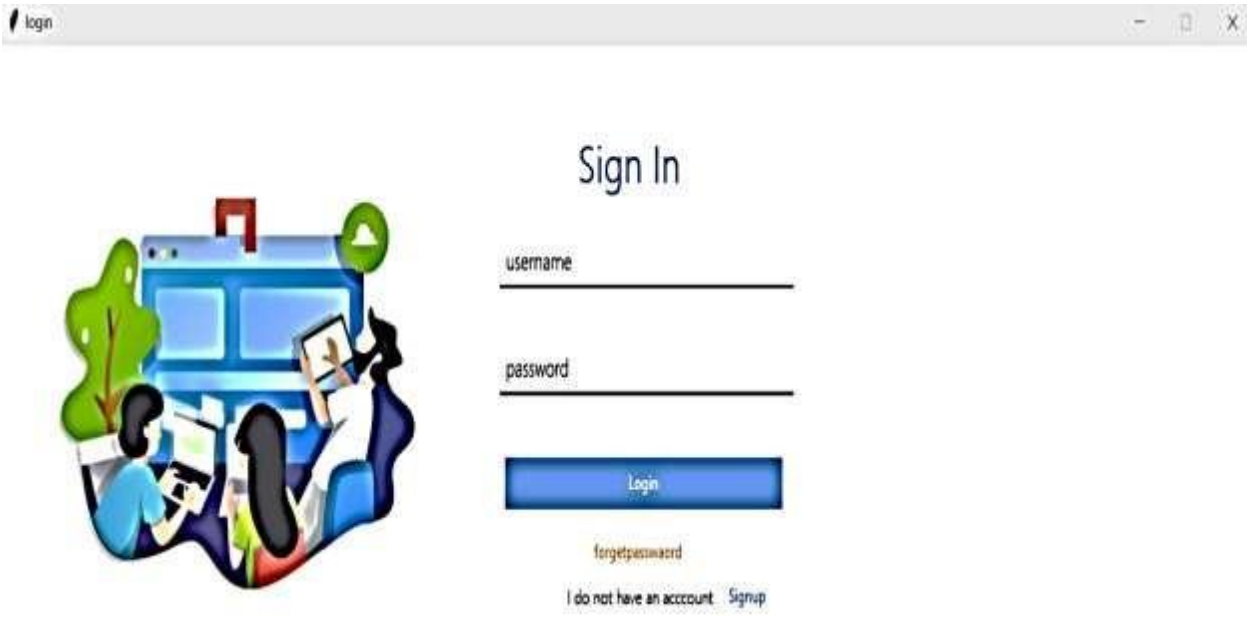

Fig:3 OUTPUT SCREEN FOR INSTITUTE OR ORGANIZATION

Fig:4 Output for students

IJESAT (Enriching the Research)
Open Access Research Article
Volume: 23 Issue: 07
July, 2023

Fig:5 Create digital signature

Fig: 6 Enter roll no and student name contact no

IJESAT
(Enriching the Research)

Open Access Research Article
Volume: 23 Issue: 07
July, 2023

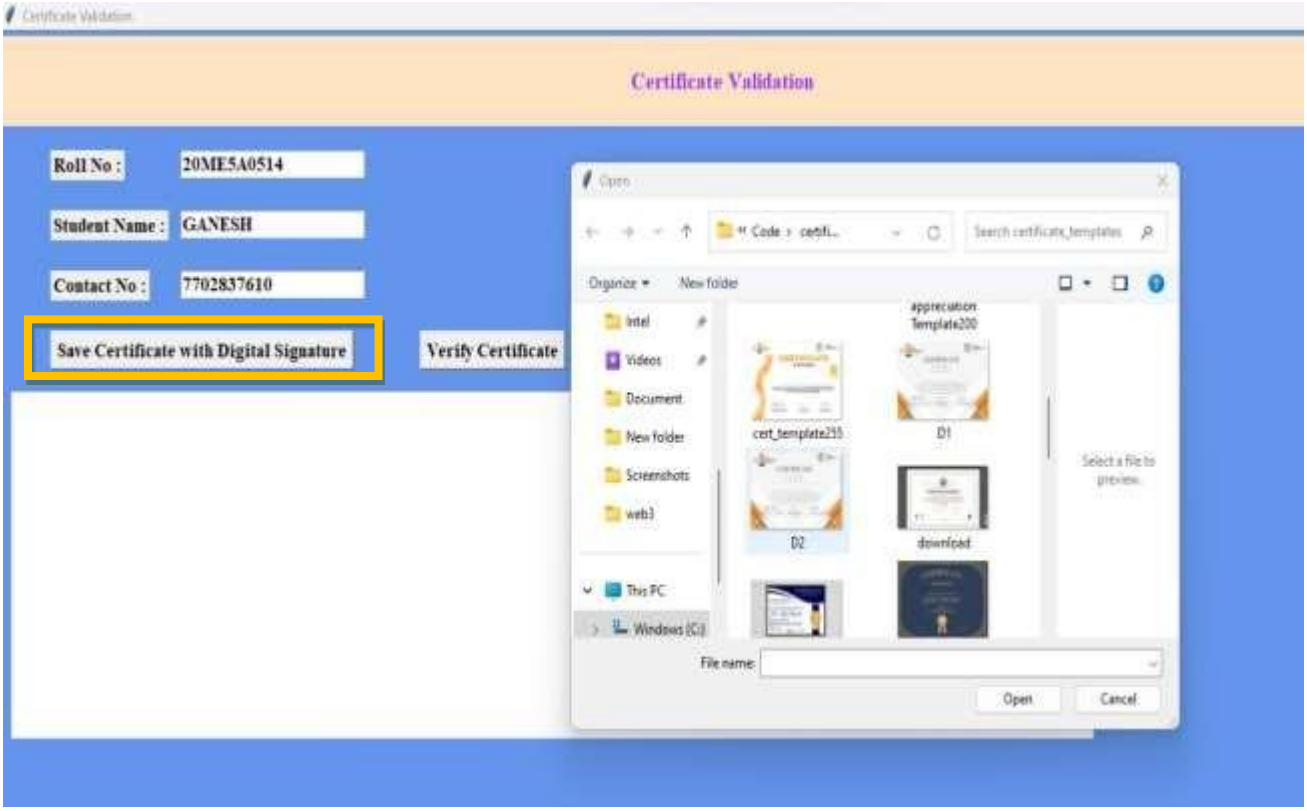

Fig: 7: Click on save certificate

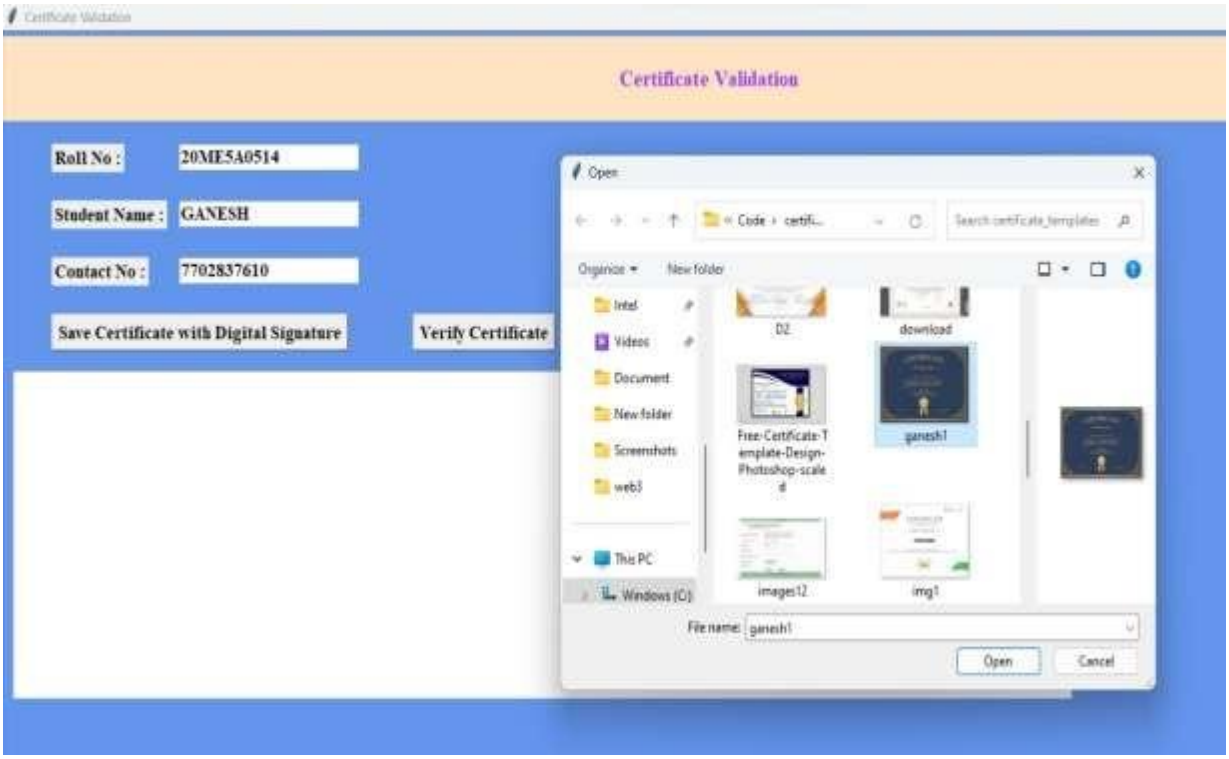

Fig: 8 Select certificates

IJESAT (Enriching the Research)
Open Access Research Article
Volume: 23 Issue: 07
July, 2023

Fig: 9 now click on “save certificate with digital signature”

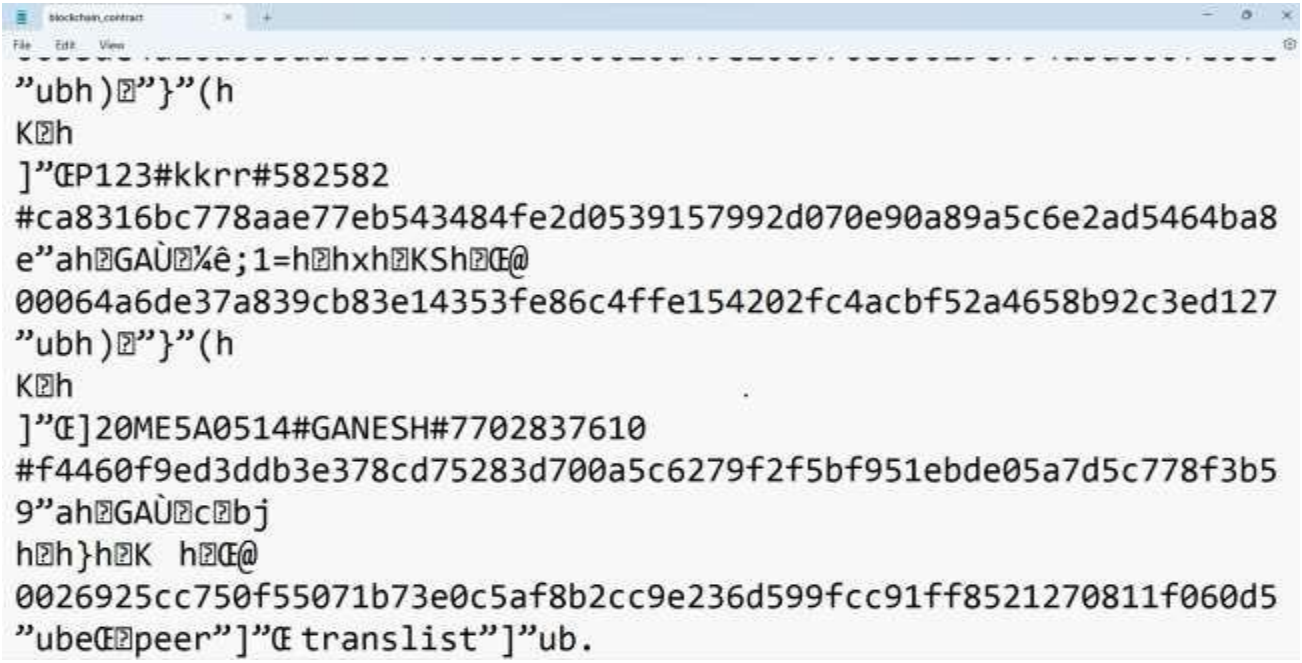

Fig: 10 the digital signature was saved in this form at local server

IJESAT
(Enriching the Research)
Open Access Research Article
Volume: 23 Issue: 07
July, 2023

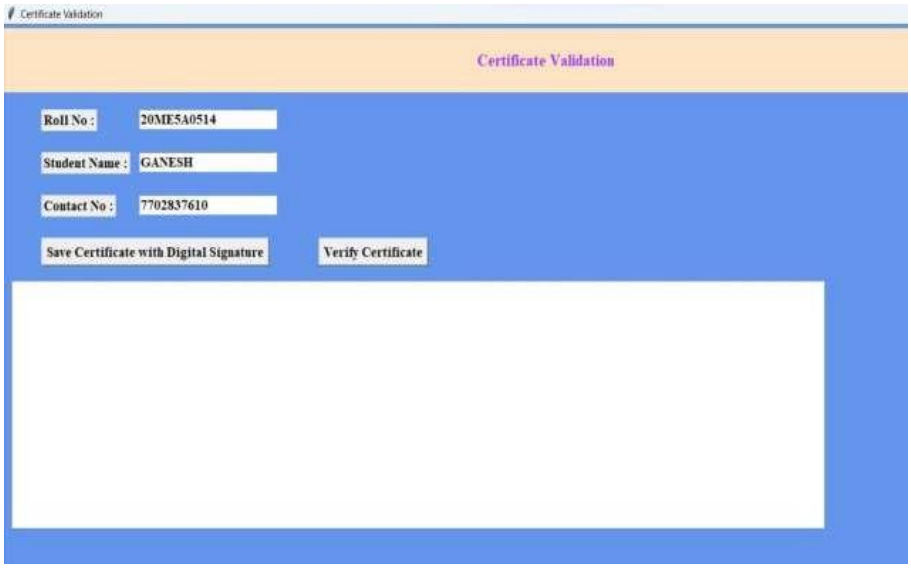

Fig: 11: Fill the roll no, student name, phone number

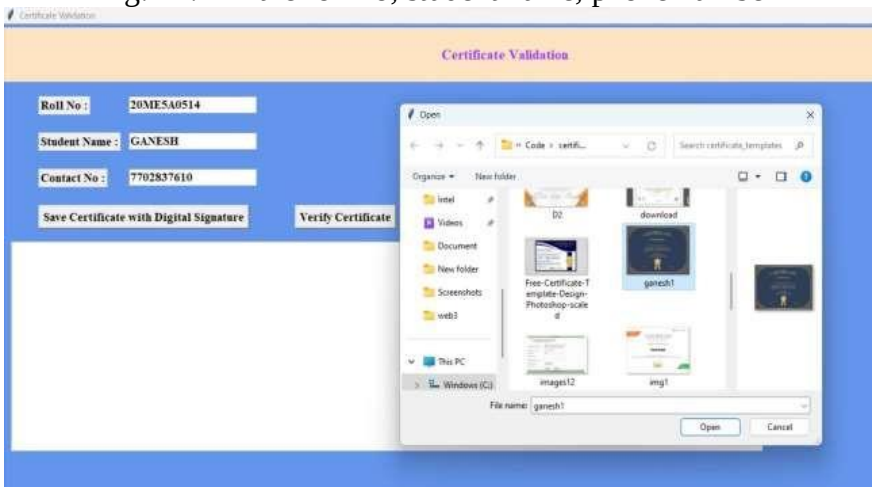

Fig: 12: Click on verify certificate

6. CONCLUSION

Certificate validation with SHA is an important part of many software projects that require secure communication between different parties. In a Python project, it is important to test the certificate validation process thoroughly to ensure that it is working as intended and is secure. Unit testing, module testing, integration testing, and acceptance testing are all important types of testing that can be used to test the certificate validation process in a Python project. These types of testing can help to identify errors or issues early in the development process

Overall, certificate validation with SHA in a Python project requires careful planning, testing, and documentation to ensure that the system is secure and functions correctly. By following best practices for testing and development, software engineers can create robust and secure systems that meet the needs of their users. Here the certificate validation with SHA is used to verify the certificates. The user can upload his certificate and create the digital signature, hash code to that certificate it was created with

IJESAT (Enriching the Research)

Open Access Research Article

Volume: 23 Issue: 07

July, 2023

the help of hashlib (SHA-256) library, he can verify the certificate with the help of digital signature. The certificate signature and hash code were stored in the database by comparing the original.

REFERENCES

1. Tengyu Yu, Blockchain operation principal analysis: 5 key technologies, iThome, https://www.ithome.com.tw/news/105374
2. JingyuanGao, The rise of virtual currencies! Bitcoin takes the lead, and the other 4 kinds can't be missed. Digital Age, https://www.bnext.com.tw/article/47456/bitc oinether-li tecoin-ripple- differences-between cryptocurrencies
3. Weiwen Yang, Global blockchain development status and trends,Benyuan He, “An Empirical Study of Online Shopping Using Blockchain Technology”, Department of Distribution Management, Takming University of Science and Technology, Taiwan, R.O.C., 2017
4. ZhenzhiQiu, “Digital certificate for a painting based on blockchain technology”, Department of Information and Finance Management, National Taipei University of Technology, Taiwan, R.O.C., 2017.
5. Yuan, Yong, and Fei-Yue Wang, "Blockchain: the state of the art and future trends," Acta Automatica Sinica 42.4 (2016): 481-494.
6. Blockchain Based Storage and Verification Scheme of Credible Degree Certificate 1 Dongwei Liu 2 Xiaojin Guo