A Privacy-Centered Protocol for Enhancing Security and Authentication of Academic Certificates

Omar S. Saleh[1], Osman Ghazali[2]*, Norbik Bashah Idris[3]
Studies-Planning and Follow-up Directorate, Ministry of Higher Education and Scientific Research, Baghdad, Iraq[1]
School of Computing, Universiti Utara Malaysia, Kedah, Malaysia[1, 2]
Kulliyyah of Information and Communication Technology, International Islamic University Malaysia,
Kuala Lumpur, Malaysia[3]

***Abstract*—Academic certificate authentication is crucial in safeguarding the rights and opportunities of individuals who have earned academic credentials. This authentication helps prevent fraud and forgery, ensuring that only those who have genuinely earned certificates can use them for education and career opportunities. With the increased use of online education and digital credentials in the digital age, the importance of academic certificate authentication has significantly grown. However, traditional techniques for authentication, such as QR code, barcode, and watermarking, have limitations regarding security and privacy. Therefore, proposing a privacy-centred protocol to enhance the security and authentication of academic certificates is vital to improve the trust and credibility of digital academic certificates, ensuring that individuals' rights and opportunities are protected. In this context, we adopted the Challenge Handshake Authentication (CHA) protocol to propose the Certificate Verification Privacy Control Protocol (CVPC). We implemented it using Python and Flask with a Postgres database and an MVT structure for the application. The results of the implementation demonstrate that the proposed protocol effectively preserves privacy during the academic certificate issuance and verification process. Additionally, we developed a proof of concept to evaluate the proposed protocol, demonstrating its functionality and performance. The PoC provided insights into the strengths and weaknesses of the proposed protocol and highlighted its potential to prevent forgery and unauthorised access to academic certificates. Overall, the proposed protocol has the potential to significantly enhance the security and authenticity of academic certificates, improving the overall trust and credibility of the academic credentialing system.**

***Keywords*—Academic certificates; privacy-centered protocol; privacy preservation; challenge handshake authentication protocol**

I. Introduction

Academic certificates are important documents that verify an individual's educational achievements and qualifications, serving as proof of their knowledge, skills, and competencies in a particular field of study. Employers, educational institutions, and other organisations often use academic certificates to evaluate an individual's qualifications for a job or further education opportunities. A study by the National Center for Education Statistics (NCES) found that in 2020, about 42% of the US population aged 25 and over had at least a bachelor's degree, which is an increase from 29% in 2000. This increase in the number of college graduates highlights the importance of academic certificates, as employers and institutions require higher levels of education and skills [1], [2], [3].

Moreover, academic certificates play a crucial role in career advancement. A study by the Georgetown University Center on Education and the Workforce revealed that a worker with a bachelor's degree earns about $1 million more in median lifetime earnings than a worker with only a high school diploma. In conclusion, academic certificates are important documents used to verify an individual's education and qualifications. They are becoming increasingly important as the number of college graduates increases, and employers and institutions require higher levels of education and skills, playing a vital role in career advancement. Academic certificate forgery is a severe issue affecting educational institutions, employers, and individuals [26], [31].

A study by the International Association for Educational Assessment (IAEA) suggests that academic certificate forgery is a growing problem worldwide, with an estimated 5-10% of all certificates being fraudulent. The rate of diploma fraud was 0.1% among the 3.5 million students whose records were checked in the United States, according to a study by the National Student Clearinghouse Research Center. The most common form of fraud was the use of a false high school diploma to gain admission to college [22]. In India, a study by the Centre for Media Studies found that up to 40% of engineering graduates in India may have fake degrees. The study revealed that many students could obtain fake degrees from unaccredited institutions or by paying bribes to officials. In China, a study by the China Academic Degrees & Graduate Education Development Center found that the rate of academic certificate forgery was about 3.15% among the population of college graduates, with most of the forgeries in the fields of engineering and medicine. While the methodologies of these studies may differ, they all suggest that academic certificate forgery is a widespread problem with severe consequences for educational institutions, employers, and society as a whole [1], [2], [3].

Therefore, it is essential for institutions and employers to have proper measures in place to detect and prevent certificate forgery to ensure that only qualified individuals are awarded and recognised for their education. Academic certificate verification is a critical process that helps mitigate the problem of academic certificate forgery by checking the authenticity of an academic certificate to ensure that a legitimate institution

*Corresponding Author.

issued it and that the individual who holds the certificate completed the coursework and earned the degree.

A graduation certificate, also known as a diploma or degree certificate, is a document awarded to a student upon successfully completing a course of study or program, including the student's name, the name of the institution, and the degree or diploma earned. It typically includes the student's grades or other academic information in some cases. It serves as official proof of the student's educational achievements and is often required for further education or employment. Some universities, colleges, and vocational schools also provide an official transcript with the graduation certificate.

However, ensuring privacy in academic certificate issuance and verification systems is a critical concern [32]. The proposed Privacy-Centered Protocol for Enhancing the Security and Authentication of Academic Certificates is based on the Challenge Handshake Authentication (CHA) protocol and offers several key contributions that could revolutionise the academic certificate issuance and verification process. Firstly, the protocol prioritises the privacy of certificate holders by ensuring that personal information is not disclosed during the verification process. Secondly, it employs the CHA protocol, which uses a challenge-response mechanism to enhance the security of academic certificates. Additionally, the protocol is tamper-proof and uses digital signatures to ensure the authenticity of certificates. It is also easily accessible to all stakeholders and compatible with commonly used devices, making it a practical solution for academic institutions. Finally, the protocol is designed to be compatible with emerging technologies such as blockchain [8], ensuring its longevity and continued relevance. Overall, the proposed protocol focuses on privacy, security, tamper-proof nature, accessibility, and compatibility, making it a promising solution for enhancing the security and authentication of academic certificates. The next subsections will discuss the importance of graduation certificates and the related security and privacy requirements.

A. Importance of a Graduation Certification Verification (GCV) System

A Graduation Certification Verification (GCV) system is of paramount importance in the modern job market and academic landscape. The system provides a reliable and secure means of verifying the authenticity of academic certificates, which is essential for employers, academic institutions, and government agencies. With the increasing prevalence of certificate fraud, a GCV system is critical for maintaining the integrity of the certification process and preventing fraud. By ensuring that only authentic certificates are accepted, a GCV system can help improve the job market's quality, reduce the risk of hiring unqualified candidates, and maintain trust in the certification process. Moreover, a GCV system can help to simplify and streamline the certification process, saving time and reducing costs for employers and academic institutions. Overall, a GCV system is essential for ensuring the accuracy and integrity of academic certificates and maintaining trust in the certification process.

B. Security and Privacy Requirements of a Graduation Certification Verification (GCV) System

A Graduation Certification Verification (GCV) system requires high security and privacy to ensure the authenticity of academic certificates. The system must protect the privacy and security of certificate holders' personal information and the confidentiality of the certificate itself. The following are some of the security and privacy requirements of a GCV system:

- Authentication and Authorisation: The GCV system must implement strong authentication and authorisation protocols to ensure that only authorised stakeholders can access and modify data [27],[28].
- Data Encryption: The system should use encryption technology to protect data in transit and at rest, ensuring that data is not accessible to unauthorised parties [26],[27],[28].
- Secure Storage: The system must use secure storage mechanisms to protect the confidentiality and integrity of the data, preventing unauthorised access and data loss.
- Privacy Protection: The GCV system must ensure that the certificate holder's personal information is protected, including their identity and other sensitive information[26],[27],[28].
- Data integrity: The system must ensure that the data stored in the system is authentic and cannot be tampered with. This can be achieved by using techniques such as digital signature, hash functions, and encryption [5].
- Non-repudiation: The system must provide a mechanism to ensure that the certificate holder cannot deny their ownership of the certificate. This can be achieved by using digital signature and public key infrastructure [6].
- Access control: The system must have a mechanism to control who can access the certificates and what they can do with them. This can be achieved by using role-based access control, access control lists, and permission-based systems [7], [28].

Ensuring security involves safeguarding user and stakeholder privacy and preventing unauthorised access, use, modification, or destruction of data to maintain information confidentiality. This defines the system's ability to provide protection [29]. Preserving privacy is widely considered to rely on access control technology, which is regarded as the most vital aspect [30]. By implementing these security and privacy requirements, a GCV system can protect the integrity of the certification process, prevent fraud, and maintain the trust of stakeholders. Implementing these requirements can also help ensure compliance with data protection regulations, such as GDPR, HIPAA, and CCPA.

II. LITERATURE REVIEW

The issuance and verification of academic certificates are critical processes in the academic world. The need for accurate, reliable, and secure verification of academic certificates has become increasingly important with the rise of online education and the prevalence of certificate fraud. This has led to the development of various techniques and technologies for academic certificate issuance and verification, which range from traditional methods to more modern and sophisticated approaches. In this literate review, we will explore the different techniques that have been proposed for academic certificate issuance and verification, including paper-based methods, electronic certificates, and digital signatures. We will examine the advantages and limitations of each approach, as well as their effectiveness in addressing the challenges of certificate fraud, privacy, and security. By understanding the various techniques and technologies used for academic certificate issuance and verification, we can gain insight into the future of this critical area of academic administration.

Traditional techniques for academic certificate issuance and verification have been used for decades, typically involving paper-based certificates and manual verification processes. While these methods have proven effective in many cases, they have limitations that have led to the development of more advanced technologies. In this literature review, we will explore the advantages and disadvantages of traditional techniques for academic certificate issuance and verification, including the use of paper-based certificates, manual verification processes, and the challenges of fraud prevention, privacy, and security.

Paper-based certificates have been the most widely used method for academic certificate issuance, and their validity has been verified by manual methods. However, this process is time-consuming, resource-intensive, and prone to error. Manual verification of certificates can be time-consuming and inefficient, and it may also require significant resources. Moreover, paper-based certificates are vulnerable to fraud, and they can be easily replicated or falsified. Despite the limitations of paper-based certificates, they are still in use, particularly in developing countries, where the lack of digital infrastructure and resources makes it difficult to implement more advanced technologies. In these situations, the use of paper-based certificates remains the only viable option, and efforts are being made to improve the security and validity of paper-based certificates.

QR codes are two-dimensional barcodes that can store large amounts of data in a small space, making them a popular choice for academic certificate issuance and verification. The use of QR codes can help to reduce the risk of fraud, simplify the verification process, and increase the efficiency of certificate issuance. QR has been used to store information such as the student's name, degree name, graduation year, and name of the University, making it easy for employers and institutions to verify the authenticity of the certificate[9],[10].

In [33], the research proposes a system for issuing degree certificates that includes a digital signature and a QR code tag. The QR code tag contains the graduate student's data, such as name, GPA, CGPA, and institution alias. The Higher Education Certificate Authentication System (HECAS) generates the digitally signed QR code, which is sent to the central HECAS server for verification. A smartphone application is required to authenticate the certificate by scanning the QR code. The proposed system aims to provide a secure and efficient way of issuing and verifying degree certificates.

In [34], the research proposes a system for real-time student identity card authentication using a QR code and a smartphone scanner. The system generates a unique QR code containing a student's matriculation number and other details, which is embedded in the identity card. A software application pre-installed in the smartphone scanner functions as a QR scanner, allowing for quick and efficient authentication. The proposed system aims to enhance the quality of authentication and overcome the problem of location and connectivity issues. The research shows that the smartphone scanner is an effective and faster means of authentication compared to other traditional means. The system offers a promising solution to the lack of innovation in information technology, particularly in developing countries like Nigeria.

In [35], the paper proposes a barcode-based academic certificate authentication system that uses cloud-based services to enhance security and accessibility. The system generates a unique barcode for each certificate, which can be scanned and verified using a mobile application. The authors suggest that the system could help reduce fraud and improve the verification process for academic certificates.

In [36], the paper presents a QR code-based certificate authentication and verification system for higher education. Barcodes are used to improve security and accessibility. The system generates a unique QR code for each certificate, which can be scanned and verified using a mobile application. The authors note that the system could help prevent the production and distribution of fraudulent certificates.

In [37], the paper proposes a barcode-based certificate verification system for distance education. Barcodes are used to improve the security and efficiency of certificate verification. The system generates a unique barcode for each certificate, which can be scanned and verified using a mobile application. The authors suggest that the system could help reduce the time and cost associated with traditional certificate verification methods.

Using QR codes for academic certificate issuance and verification can pose some risks in terms of privacy and security. While QR codes offer a convenient and efficient way to verify certificates, they can also contain sensitive information that could be at risk of data breaches, hacking or misuse. For example, if the QR code contains personal data such as a student's academic history, it could be used for discriminatory purposes if it falls into the wrong hands. Moreover, QR codes can be easily replicated, potentially leading to fraudulent certificates being produced. To address these issues, it is important to take appropriate security measures such as encryption, access controls, and data privacy policies. Institutions or organisations may also need to use other technologies and methods to supplement QR codes, depending on their specific requirements [11], [12], [13], [14].

In [38], the researchers proposed a verification system based on watermarking that uses a combination of visible and invisible watermarks to authenticate digital certificates. The system uses an encryption scheme based on a secret key to ensure the security of the embedded watermark and employs a unique identifier to prevent the certificate from being duplicated. The system was tested on a sample set of certificates and demonstrated high accuracy in verification.

In [39], the researchers proposed a certificate verification system that uses a combination of QR codes and watermarks. The system embeds a unique watermark into each certificate that can be used to verify its authenticity. The system also includes a QR code that can be scanned to access additional information about the certificate holder. The system was tested on a sample set of certificates and showed high accuracy in verification.

While watermarking can offer a secure method for academic certificate issuance and verification, there are still potential drawbacks in terms of privacy and security. One of the main concerns is that someone with the right tools and knowledge can remove or alter watermarks, leading to fraudulent certificates being produced. Moreover, watermarking could lead to the possibility of certificate forgery, as attackers may be able to replicate the watermark and create counterfeit certificates. Embedding watermarks may also raise concerns regarding data privacy since the watermarks may contain personal information that could be accessed or misused. Therefore, it is important to complement watermarking techniques with additional security measures, such as encryption, access controls, and policies to protect the privacy of personal data.

In [40], the researchers proposed an RFID-based certificate verification system that uses a combination of hardware and software components. Each certificate is equipped with an RFID tag that contains a unique identifier and other relevant information. When the certificate is presented for verification, an RFID reader scans the tag and sends the data to a central server, which validates the information and returns a response indicating the certificate's authenticity. The system was tested on a sample set of certificates and showed high accuracy in verification.

In [41], the researchers proposed an RFID-based verification system that uses a unique identifier and a cryptographic key to authenticate digital certificates. The system employs an RFID reader to scan the certificate and transmit the data to a central server, which uses the cryptographic key to verify the authenticity of the certificate. The system was tested on a sample set of certificates and showed high accuracy in verification. The researchers also noted that the use of RFID technology can help prevent certificate fraud since the RFID tag is difficult to replicate or alter without the proper tools and knowledge.

However, there are potential drawbacks to using RFID technology for academic certificate issuance and verification. One concern is that the use of RFID technology could result in unauthorised access to personal data since the RFID tag contains sensitive information. Attackers may use unauthorised RFID readers to intercept the data or copy the RFID tag's content. Furthermore, the use of RFID technology may raise concerns about data protection and privacy since RFID tags are capable of tracking individuals and monitoring their movements. Additionally, the cost of implementing RFID technology may be higher than other methods, which could be a barrier to adoption for some institutions. Therefore, it is essential to take appropriate measures to protect the privacy of personal data and prevent unauthorised access or interception of the RFID data.

However, watermarking relies on the visibility of the watermark, which can be difficult to detect in low-resolution images and can be removed through image manipulation [15], [16]. Table I shows the comparison between QR-Code, Barcode, watermarking and RFID.

TABLE I. COMPARISON BETWEEN QR-CODE, BARCODE, WATERMARKING AND RFID

Technique	Advantages	Disadvantages	References
QR Code	Can be read quickly and easily using a smartphone camera; Can store a large amount of data in a small. Can be easily integrated into existing systems.	Can be easily replicated or forged. Can be easily damaged or obscured, making it difficult to read.	[17], [18], [19]
Barcode	Can be read quickly and easily using a barcode scanner. Can store a limited amount of data in a small space. Can be easily integrated into existing systems.	Can be easily replicated or forged. Can be easily damaged or obscured, making it difficult to read.	[17], [18], [19]
Watermarking	Can be used to embed hidden information in the certificate that can be used to verify authenticity. Can be difficult to replicate or forge.	Can be easily damaged or obscured, making it difficult to read. Can be computationally expensive to create and verify.	[17], [18], [19]
RFID	Can be read quickly and easily using an RFID reader. Can store a large amount of data in a small space. Can be used for contactless authentication.	Can be easily replicated or forged. Can be easily damaged or obscured, making it difficult to read. Can be expensive to implement and maintain.	[17], [18], [19]

III. THE PROPOSED DESIGN OF CENTRALIZED CERTIFICATE VERIFICATION PRIVACY CONTROL PROTOCOL (CVPC PROTOCOL)

The proposed design of the Centralized Certificate Verification Privacy Control (CVPC) protocol aims to address the shortcomings of traditional techniques such as QR codes, barcodes, watermarking and RFID for academic certificate issuance and verification. The CVPC protocol utilises a centralised server for certificate issuance and verification, which is responsible for maintaining the integrity and authenticity of the certificates. This centralised server is

responsible for generating and issuing digital certificates, as well as verifying the authenticity of the certificates when requested. The CVPC protocol utilises a combination of advanced cryptographic techniques, such as digital signatures and hash functions, to ensure the integrity and authenticity of the certificates. The digital certificates are issued with a unique digital signature, which is generated by the centralised server using the private key of the issuing institution. The digital signature ensures that the certificate has not been tampered with or modified in any way. The CVPC protocol also utilises a unique identification number, which is embedded in the digital certificate and is used to verify the authenticity of the certificate. This identification number is generated by the centralised server and is based on the student's personal information, such as their name, date of birth, and the institution they graduated from. The CVPC protocol also includes a privacy-preserving mechanism, which allows the student to control who has access to their personal information and the digital certificate. The student is provided with a private key, which is used to encrypt the personal information and digital certificate. The private key is stored on the student's device and is only accessible by the student.

With this proposed solution, three main objectives were sufficed. Primarily:

- The privacy aspect. The student can lock and unlock their certificates.
- Only authorised entities can exist in the system with sufficient authorisation and access control.
- Timely verification of certificates by third parties.

From the previous details, privacy was a major drawback in most of the existing solutions when it came to certificate verification. The process itself is quite troublesome, especially for verifiers. The first components towards sufficing the objectives of this research start with developing a privacy-first solution that allows the user to control how the public views the certificate in a centralised environment. Fig. 1 shows the design for the proposed centralised certificate verification privacy control protocol.

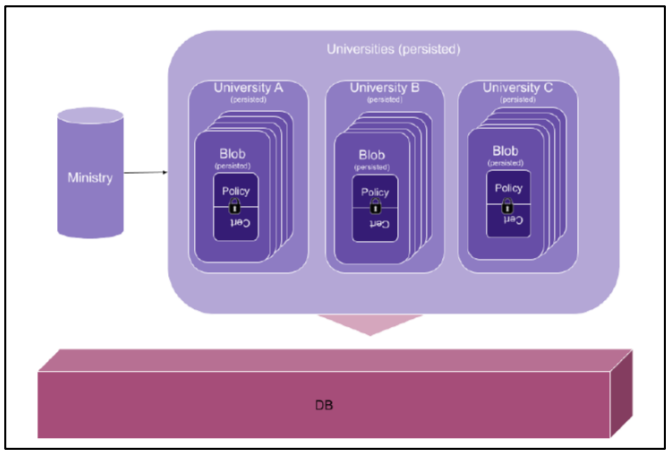


Fig. 1. The proposed centralised certificate verification privacy control protocol.

The number of ministries in the world is finite n(Ministry) = x,{ x=constant | x>0} and usually there is one per country Ministryx⊂Countryx which is usually responsible for the quality of education in their respective countries. The ministry of education can go under different names like the case of Mexico it is called Secretariat of Public Education [16]. Nevertheless, this should not have any impact on the design since the ministry is an entity that controls and generates universities {$University_1$,....,$University_n$} ∈Ministryx | n=>1. The set of ministries based on the proposition above is finite hence they are hard coded into the system (by their official admin emails); Each Ministry is able to only create universities in the system. Each university is created by one and only one ministry. For the cases where there are different branches of a single university in different countries, this would neither be impacted nor will it cause the system to behave wrongly. For example, Birmingham University, originally situated in the UK and precisely England, would be created by the Ministry of Education in the UK. Birmingham University also has a branch in Malaysia. The Malaysian Ministry of Education would create the latter. Each university issues its own certificates. However, in the proposed solution, as a certificate is generated a privacy policy is also generated and attached to that generated certificate as shown in the design Fig. 1. By default, the certificate is locked, which means any third party attempting to view the certificate will not be able to see its details. When the university creates a certificate, another task is triggered in the background, generating a student for that certificate. The way this is achieved is by using the registered email of the student in that university. This is to suffice for authentication. The student would get an activation token that allows them access to the certificate and policy. The student after activating their account would be able to control how each piece of information is displayed to third parties. The mechanism used to achieve the above is an adaptation from the Challenge Handshake Authentication Protocol (CHAP) which is shown in Fig. 2. CHAP suffices when a link is between a server and a client [20],[23,[24].

- The server sends a challenger message to the client.
- The client responds.
- The server checks if the response matches the expected value, then the authentication is acknowledged, and the connection happens otherwise it is terminated.

The Challenge Handshake Authentication protocol was adopted in the proposition of the certificate verification privacy control protocol (CVPC). CHAP operates by first establishing a connection between the user and the network resource. The network resource then sends a challenge message to the user, typically a random string of characters or a nonce, which the user must use to generate a response message. The user generates the response by running a one-way hash function on the challenge message using a shared secret key known only to the user and the network resource. The resulting hash value is then sent back to the network resource, which compares it to its own calculation of the expected response. If the two values match, the user is authenticated and granted access to the network resource. Details are shown in the next section. The Challenge Handshake Authentication Protocol (CHAP)

proposed by [20],[21], which was discussed in the previous section, was adopted in that same manner in the CVPC protocol. It is used when a ministry adds a university, and a university issues a certificate and assigns a student. The adoption and the implementation of Challenge Handshake Authentication protocol (CHAP) in academic certificates verification use case is given in Fig. 3. It shows how the relationship between the university and the students.

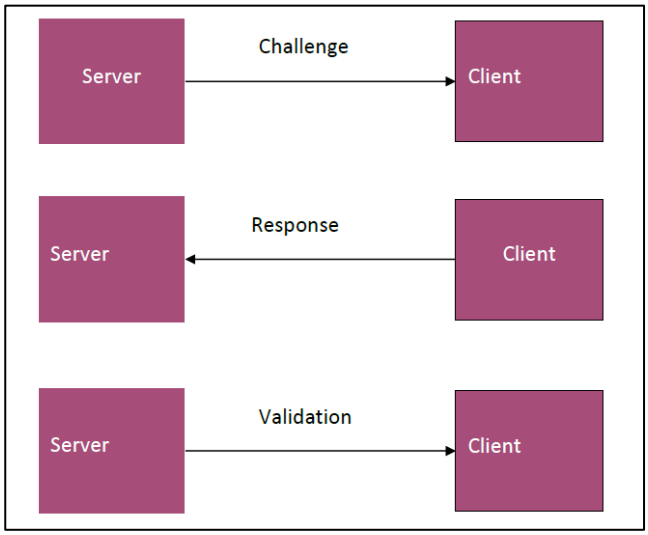


Fig. 2. Challenge Handshake Authentication Protocol (CHAP).

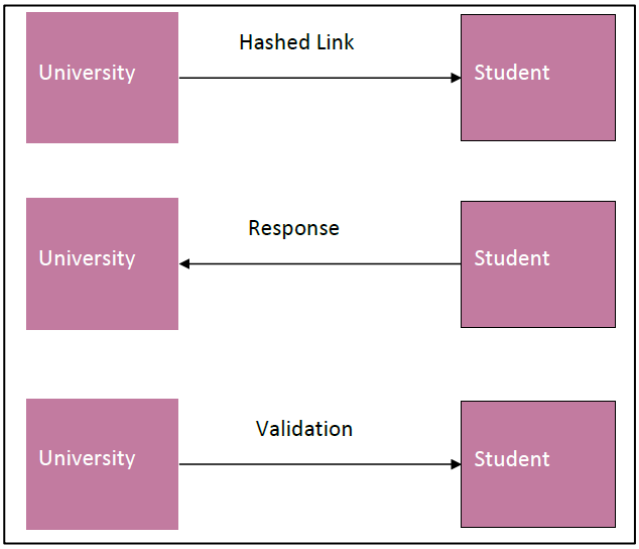


Fig. 3. Implmentation of Challenge Handshake Authentication Protocol (CHAP) in academic certificates verification use case.

The proposed CHAP Certificate Verification Privacy Control Protocol used is based on the following steps:

Step 1: A request is sent to the student's email. The request is in the form of a signed link that is specific to that student, and the link contains a token. The token results from hashing of a user's identifier with the student's email and a timestamp. The timestamp is important to validate the lifespan of the link. The link is meant to be active for a pre-defined period of time to minimise hanging certificates. Meaning certificates in the system without confirmed students.

Step 2: The students from their official emails access the link supplied. This step acts as a response to the request sent by the server. It is important to note that each link is unique to the student and can only be accessed from their official email, which requires authorisation and access control.

Step 3: The server validates the authenticity of the token sent by the student by decrypting it and retrieving the email address hashed in the token, using the same student identifier that was used to sign the token. If the token is valid, the student is directed to the certificate and policy and can unlock the certificate.

The proposed protocol uses HMAC and SHA-512 to sign the hashed link. HMAC stands for Keyed-Hashing for Message Authentication and is a widely used message authentication code based on cryptographic hash functions like MD5 and SHA-1. The student identifier acts as a namespace for the URL and is unique to each student. Therefore, the student identifier is usually the student's username or ID. This adds an extra layer of privacy since no two tokens can be decrypted using the same parameters. Since each email and student identifier is unique, each link is specific to a single student.

Based on what has been discussed in the previous section the following protocol is proposed (CVPC protocol).

Step 1: The ministry adds a university using CCVPC proposed ,CCVPC(University) ∈ Ministry.

Step 2: The university adds students using CCVPC, University → CCVPC(Studentn), n ∈ list of students in university.

Step 3: The university issues certificates with Privacy Policy, University → PsxCs, P=Policys, C=Certificates, s={Student0,....,Studentn}.

Step 4: Privacy Policy adds a layer of protection to the Certificates Ps(Cs).

Step 5: All inbound traffic hits the Privacy Policy first. Inboundrequest → Ps → Cs.

Step 6: Student lock/Unlock their certificates sufficing privacy L(Cs), U(Cs), L=Lock, U= Unlock.

Step 7: Students share ids of certificates with the third parties and based on the privacy policy they are able to see the information T(PsCs) ∋Studentn⇒ U(Cs), T=Third party.

IV. The Proposed Verification of Certificates by Third Parties

The third party can simply use a fixed id supplied by the student to access the certificate and validate the information. T(PsCs) ∋Studentn → U(Cs), T=Third party, Ps=Student Policy, Cs= Student Certificate, U= Unlocking.

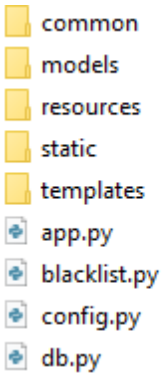
The student can after being authorised into the system using the CCVPC proposed will be able to control each element of his/her certificate. Such that.

Studentn → L(Cei), ei∈ Certificates | Student=Studentn where.

*ei*represents several elements like the GPA, transcript and other necessary information that is issued with the certificate. The CCVPC is a component of the proposed centralised certificate verification privacy protocol. This design ensures that the system remains free of unwanted parties. Access control is managed by authorised entities, each of which has their own control rights in the system. For example, universities issue certificates, but can only participate in the system through ministries. This control mechanism ensures proper authorisation, verification, and limits fraud. In addition, the CCVPC protocol ensures privacy by controlling who has access to the L(Cs) and U(Cs) of certificates - only the students themselves have this access. Thanks to the CCVPC protocol, no unauthorised entities can exist within the system.

V. Implementation and Results

The proposed design was implemented in Python, a widely-used programming language that is particularly effective for large-scale web applications. The web framework Flask was used with Python, while the database was implemented with Postgres, an open-source database that natively supports JSON objects. The application was structured according to the MVT architecture, which stands for Models, Views, and Templates. Models describe the database, while Views implement the business logic, and Templates provide the front-end interface with HTML and CSS. In the following subsections, we will explore the different layers of the application in more detail.



A. The Model Layer

The model folder contains all the entity models that were defined. These models represent the various actors involved in the use case, with the exception of the third party. Since third parties do not require an identity in the system, they can simply use the ID provided by the student to facilitate the verification process. In this process, several actors are involved, including the ministry, the university, students, and third parties. The ministry's responsibility is to add universities to the system, while the university takes charge of certificate issuance. Students have the ability to lock and unlock their certificates for privacy preservation. Finally, third parties are responsible for verifying the certificate. In the proposed protocol design, there are several actors involved, as depicted in Fig. 4. Additionally, this research includes the implementation of the Ministry class in Python, as demonstrated in Fig. 5.

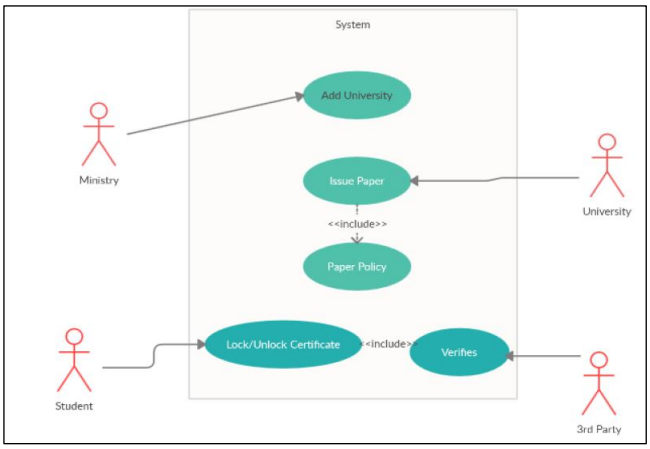


Fig. 4. Actors involved in the proposed protocol.

```
class MinistryModel(db.Model):
    __tablename__ = "ministries"
    __table_args__ = (UniqueConstraint("id"),)
    id = db.Column(db.Integer, primary_key=True)
    is_verified = db.Column(db.Boolean, default=False)
    name = db.Column(db.String(120), unique=True)
    country = db.Column(db.String(120), unique=True)
    password = db.Column(db.String(128))
```

Fig. 5. The implementation of the ministry class in python.

The same principle applies to both universities and students, with an additional class of permissions that facilitates control over the privacy of certificates. This permission class is linked to the student class through the use of student IDs.

B. The View Layer

The logic that connects the front end to the model layer is implemented in this layer. Specifically, the ministry resource includes the following resources:

- Ministry(Resource).
- MinistryRegistration(Resource).
- MinistryList(Resource).

Each of the resources listed above serves a specific purpose. For example, the ministry resource exposes an API call that returns details about the iininistry associated with a given email address.

- class Ministry(Resource):
- def get(self, email):
- email = email.lower().strip().
- Ministry = MinistryModel.find_by_email(email).
- if Ministry:
- return Ministry.json().
- return {"message": "Ministry not found"},

The Ministry Registration resource takes in the necessary information to create a new ministry. The creation of a ministry is pre-defined. The pre-defined entities are added using the post method exposed by the Ministry Registration resource above. The last Resource MinistryList(Resource) allows super admin to list existing ministries or it can also serve the general query the list of ministries registered in the system.

C. Application Front End Layer

The student is able to control the permission using the endpoint /permissions/<int:student_id>.

In this section, the proposed system's app screens illustrate various tasks, including adding a university to the system, the university's view for adding a certificate, the student's view for managing permissions, and the third-party's view of the application. Fig. 6 displays a screenshot of the university addition process, while Fig. 7 showcases a screenshot of the university adding a certificate. Furthermore, Fig. 8 demonstrates how a student can preserve their privacy. The student view for managing permissions is shown in Fig. 9, which displays a screenshot of a third-party verifying a certificate shared by the student.

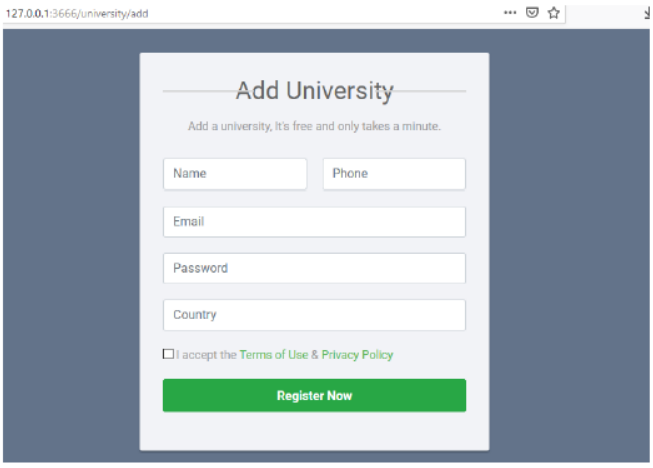


Fig. 6. Screenshot of adding a university.

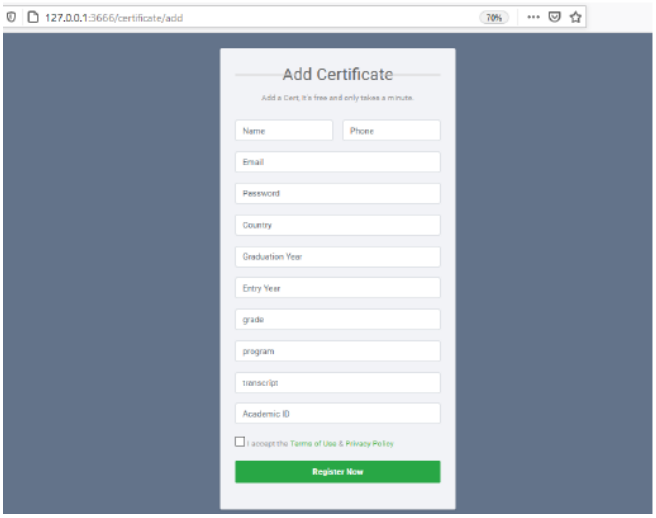


Fig. 7. Screenshot of adding a certificate by the university.

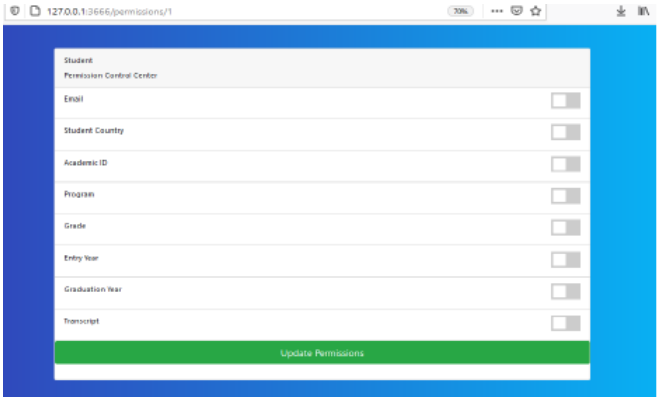


Fig. 8. Screenshot of how a student can preserve their privacy.

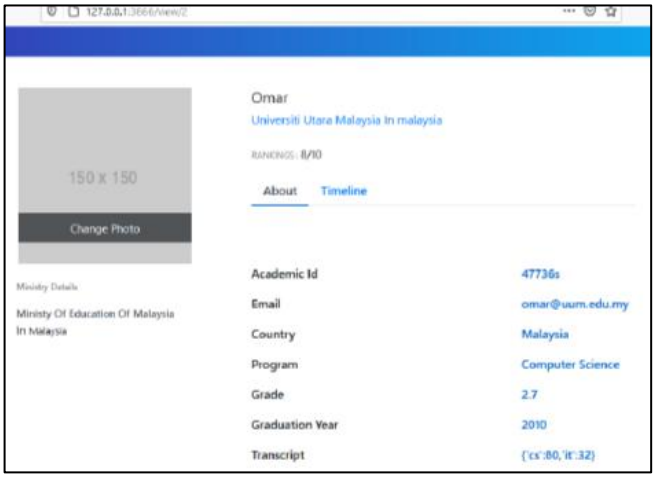


Fig. 9. Screenshot of third-party verifying the certificate shared by the student.

VI. Discussion

The Privacy-Centered Protocol for Enhancing the Security and Authentication of Academic Certificates based on the Challenge Handshake Authentication (CHA) protocol has the potential to significantly enhance the security and authenticity of academic certificates. The protocol's key contributions, including its focus on privacy, tamper-proof nature, and compatibility with emerging technologies, make it a promising solution for academic institutions. One of the most significant benefits of the proposed protocol is its emphasis on privacy. The protocol ensures that personal information is not disclosed during the verification process, providing an extra layer of protection to certificate holders. This privacy-centric approach is essential in today's digital age, where data breaches and identity theft have become significant concerns for individuals and organisations alike. Another significant advantage of the proposed protocol is its tamper-proof nature. The use of digital signatures ensures the authenticity and integrity of academic certificates, making it easy to detect fraudulent certificates. This tamper-proof nature can significantly enhance the overall trust in the academic certificate issuance and verification process, providing a more secure means of verifying academic credentials. The protocol's compatibility with emerging technologies such as blockchain is also noteworthy. The integration with blockchain technology can further enhance the

security and reliability of academic certificate verification. Blockchain technology provides a decentralised and tamper-proof way of storing and verifying data, making it an ideal solution for enhancing the security and authenticity of academic certificates. Despite the potential benefits, the adoption of the proposed protocol may face challenges. One of the challenges is the adoption and integration of the protocol into existing systems. It may require significant changes to the existing infrastructure and systems, which can be time-consuming and costly. Additionally, compatibility with emerging technologies such as blockchain requires a certain level of technical expertise, which may be a barrier to some organisations. In conclusion, the Privacy-Centered Protocol for Enhancing the Security and Authentication of Academic Certificates based on the CHA protocol is a promising solution for enhancing the security and authenticity of academic certificates. The protocol's emphasis on privacy, tamper-proof nature and compatibility with emerging technologies makes it a practical and robust solution for academic institutions. While there may be challenges to its adoption, the benefits of adopting the protocol far outweigh the potential challenges, providing a more secure and reliable means of verifying academic credentials.

VII. Benefits of Privacy Centralised Verification Control Protocol for Academic Certificates Issuance and Verification

Proposing a new privacy-centralised verification control protocol for academic certificates issuance and verification is important for several reasons [25], including:

- Security: Traditional methods of academic certificate authentication, such as QR code and barcode, are vulnerable to tampering and replication. A new privacy-centralised verification control protocol can enhance the security of the certificate verification process by incorporating advanced security techniques such as digital signature, encryption, and biometrics.
- Privacy: Centralised certificate verification systems can be a potential privacy breach, as they can expose the personal information of certificate holders to unauthorised access. The new privacy-centralised verification control protocol aims to preserve the privacy of the certificate holders by implementing a privacy-preserving protocol that protects the personal information of the certificate holders from unauthorised access.
- Scalability: The proposed protocol can handle a large number of requests and users, which is crucial in today's digital era where the use of digital credentials has increased.
- Compliance: The proposed protocol can ensure compliance with various privacy regulations and standards, such as GDPR, which is increasingly important as organisations have to comply with more stringent regulations to protect personal data.

In summary, proposing a new privacy-centralised verification control protocol for academic certificate issuance and verification is crucial to ensure the security, privacy and scalability of the system, as well as to provide an efficient user experience and compliance with regulations.

VIII. Evaluation of the Proposed Protocol

Evaluating a proposed design of the Centralized Certificate Verification Privacy Control Protocol (CVPC Protocol) is crucial to ensure its effectiveness and efficiency in improving the security and privacy of academic certificate authentication. One way to evaluate the proposed protocol is by developing a proof of concept (PoC) and testing it with real-world scenarios and data. The PoC can be used to demonstrate the functionality and performance of the proposed protocol and provide insights into its strengths and weaknesses. The PoC development process can involve several steps, such as designing the system architecture, implementing the proposed security measures and privacy-preserving protocols, and testing the system with simulated or real-world data. The PoC can be evaluated based on various performance metrics, such as security, privacy, scalability, and usability. For example, the security of the proposed protocol can be evaluated by assessing its resistance to various security threats, such as tampering and replication. The proposed protocol's privacy can be evaluated by examining its compliance with various privacy regulations and standards, such as the General Data Protection Regulation (GDPR). Similarly, the protocol's scalability can be evaluated by assessing its capacity to accommodate a significant number of requests and users. Additionally, the usability of the proposed protocol can be evaluated by analysing its user interface and user experience.

IX. Conclusion

In conclusion, the proposed Design of Centralised Certificate Verification Privacy Control Protocol (CVPC Protocol) addresses the need for improved security and privacy in the realm of academic certificate authentication. The implementation of the proposed protocol involved the use of several technologies, including Python, Flask, and a Postgres database, as well as the utilisation of an MVT structure. Through the utilisation of these technologies and methodology, the proposed protocol has effectively demonstrated the preservation of privacy throughout the academic certificate issuance and verification process. A proof of concept was developed to further validate the functionality and performance of the protocol, which revealed its potential to prevent certificate forgery and unauthorised access. The CVPC Protocol proposed presents a promising solution for improving the security and privacy of academic certificate authentication. Future work involves building the protocol based on a blockchain platform.

Acknowledgment

This research was supported by Ministry of Higher Education (MoHE) of Malaysia through Fundamental Research Grant Scheme (FRGS/1/2018/ICT04/UUM/02/17).

References

[1] Rios, J. A., Ling, G., Pugh, R., Becker, D., & Bacall, A. (2020). Identifying critical 21st-century skills for workplace success: A content analysis of job advertisements. Educational Researcher, 49(2), 80-89.

[2] Protopsaltis, S., & Baum, S. (2019). Does online education live up to its promise? A look at the evidence and implications for federal policy. Center for Educational Policy Evaluation, 1-50.

[3] Abelha, M., Fernandes, S., Mesquita, D., Seabra, F., & Ferreira-Oliveira, A. T. (2020). Graduate employability and competence development in higher education—A systematic literature review using PRISMA. Sustainability, 12(15), 5900.

[4] Eaton, S. E., & Carmichael, J. J. (2023). Fake degrees and credential fraud, contract cheating, and paper mills: Overview and historical perspectives. Fake Degrees and Fraudulent Credentials in Higher Education, 1-22.

[5] M. Gariup and J. Piskorski, "The challenge of detecting false documents at the border: Exploring the performance of humans, machines and their interaction," *International Journal of Critical Infrastructure Protection*, vol. 24, pp. 100–110, 2019, doi: 10.1016/j.ijcip.2018.10.005.

[6] J. K. Adjei *et al.*, "Document Authentication System Preventing and Detecting Fraud of Paper Documents," *ProQuest Dissertations and Theses*, vol. 5, no. 2, pp. 58–63, 2014, doi: http://dx.doi.org/10.1108/AP-05-2012-0049.

[7] N. Massing and S. L. Schneider, "Degrees of competency: the relationship between educational qualifications and adult skills across countries," *Large Scale Assess Educ*, vol. 5, no. 1, Dec. 2017, doi: 10.1186/s40536-017-0041-y.

[8] E. Tijan, S. Aksentijević, K. Ivanić, and M. Jardas, "Blockchain technology implementation in logistics," *Sustainability (Switzerland)*, vol. 11, no. 4. MDPI, Feb. 01, 2019. doi: 10.3390/su11041185.

[9] G. Grolleau, T. Lakhal, and N. Mzoughi, "An introduction to the Economics of Fake Degrees," *J Econ Issues*, vol. 42, no. 3, pp. 673–693, 2008, doi: 10.1080/00213624.2008.11507173.

[10] Aini, Q., Rahardja, U., Tangkaw, M. R., Santoso, N. P. L., & Khoirunisa, A. (2020). Embedding a blockchain technology pattern into the QR code for an authentication certificate. Jurnal Online Informatika, 5(2), 239-244.

[11] Suteja, B. R., Imbar, R. V., & Johan, M. C. (2020). e-Certificate system based on Portable Document Format and QR Code for Academic Activities. International Journal of Computer Science Issues (IJCSI), 17(6), 87-91.

[12] Mayowa, O. O., Adedayo, E. W., Olamide, O. O., Awokola, J. A. P., & Sodipo, Q. B. (2021). Design and Implementation of a Certificate Verification System using Quick Response (QR) Code. LAUTECH JOURNAL OF COMPUTING AND INFORMATICS, 2(1), 35-40.

[13] Mayowa, O. O., Adedayo, E. W., Olamide, O. O., Awokola, J. A. P., & Sodipo, Q. B. (2021). Design and Implementation of a Certificate Verification System using Quick Response (QR) Code. LAUTECH JOURNAL OF COMPUTING AND INFORMATICS, 2(1), 35-40.

[14] Chanda, D. (2019). Barcode Technology and its Application in Libraries. Akanbi, LM, Bashorun, MT, Salihu, UA, Babafemi, GO, Sulaiman, K., & Kolajo, SO (2019). Application of Barcode Technology in Landmark University Centre for Learning Resources, Omu-Aran Experience. Library Philosophy and Practice (e-Journal). Retrieved from http://digitalcommons. unl. ed.

[15] Ray, A., & Roy, S. (2020). Recent trends in image watermarking techniques for copyright protection: a survey. International Journal of Multimedia Information Retrieval, 9(4), 249-270.

[16] VELIČKOVIĆ, Z., VELIČKOVIĆ, S., & MILIVOJEVIĆ, Z. (2021). „Application of Watermark in the Form of QR Code in COVID Certificate Validation “. Journal of Mechatronics, Automation and Identification Technology JMAIT, 6(2), 1-5.

[17] Agrahari, A. K., & Varma, S. (2021). A provably secure RFID authentication protocol based on ECQV for the medical internet of things. Peer-to-Peer Networking and Applications, 14(3), 1277-1289.

[18] Calderoni, L., & Maio, D. (2020, September). Lightweight Security Settings in RFID Technology for Smart Agri-Food Certification. In 2020 IEEE International Conference on Smart Computing (SMARTCOMP) (pp. 226-231). IEEE.

[19] 13 Khan, R. A., & Lone, S. A. (2021). A comprehensive study of document security system, open issues and challenges. Multimedia Tools and Applications, 80(5), 7039-7061.

[20] Sale, O. S., Ghazali, O., & Al Maatouk, Q. (2019). Graduation certificate verification model: a preliminary study. International Journal of Advanced Computer Science and Applications, 10(7).

[21] Otuya, J. A. (2019). A Blockchain approach for detecting counterfeit academic certificates in Kenya (Doctoral dissertation, Strathmore University).

[22] González-Gaudiano, E. J., Meira-Cartea, P. Á., & Gutiérrez-Bastida, J. M. (2020). Green Schools in Mexico and Spain: Trends and Critical Perspective. In Green Schools Globally (pp. 269-287). Springer, Cham.

[23] Hussein, K. Q. (2019). Client Authentication By Selected Secure Password-Based On Image Using Challenge Handshake Authentication Protocol. Iraqi Journal of Information Technology. V, 9(3), 2018.

[24] Ibrahim, A. S., & Hussein, K. Q. (2019). Client authentication by selected secure password-based on image using challenge handshake authentication protocol. Iraqi Journal of Information Technology.

[25] Ayub Khan, A., Laghari, A. A., Shaikh, A. A., Bourouis, S., Mamlouk, A. M., & Alshazly, H. (2021). Educational Blockchain: A Secure Degree Attestation and Verification Traceability Architecture for Higher Education Commission. Applied Sciences, 11(22), 10917.

[26] Saleh, O. S., Ghazali, O., & Rana, M. E. (2020). Blockchain based framework for educational certificates verification. Journal of critical reviews, 7(3), 79-84.

[27] Saleh, O. S., Ghazali, O., & Idris, N. B. (2021, January). A New Decentralized Certification Verification Privacy Control Protocol. In 2021 3rd International Cyber Resilience Conference (CRC) (pp. 1-6). IEEE.

[28] Din, I. U., Hassan, S., Almogren, A., Ayub, F., & Guizani, M. (2020). PUC: Packet update caching for energy efficient IoT-based information-centric networking. Future Generation Computer Systems, 111, 634-643.

[29] Hashim, N. L., Yusof, N., Hussain, A., & Ibrahim, M. (2022). User experience dimensions for e-procurement: A systematic review. Journal of Information and Communication Technology, 21(4), 465-494. https://doi.org/10.32890/jict2022.21.4.1

[30] Din, I. U., Guizani, M., Kim, B. S., Hassan, S., & Khan, M. K. (2018). Trust management techniques for the Internet of Things: A survey. IEEE Access, 7, 29763-29787.

[31] Eaton, S. E., & Carmichael, J. J. (2023). Fake degrees and credential fraud, contract cheating, and paper mills: Overview and historical perspectives. Fake Degrees and Fraudulent Credentials in Higher Education, 1-22.

[32] Pathak, S., Gupta, V., Malsa, N., Ghosh, A., & Shaw, R. N. (2022). Blockchain-Based Academic Certificate Verification System—A Review. Advanced Computing and Intelligent Technologies: Proceedings of ICACIT 2022, 527-539.

[33] Ahmed, H. A., & Jang, J. W. (2017). Higher educational certificate authentication system using QR code tag. Int. J. Appl. Eng. Res, 12(20), 9728-9734.

[34] Emmanuel, A. A., Adedoyin, A. E., Mukaila, O., & Roseline, O. O. (2020). Application of smartphone qrcode scanner as a means of authenticating student identity card. International Journal of Engineering Research and Technology, 13(1), 48-53.

[35] Abbas, A. A. (2019). Cloud-based framework for issuing and verifying academic certificates. Int. J. Adv. Trends Comput. Sci. Eng, 8(6), 2743-2749.

[36] Singhal, A., & Pavithr, R. S. (2015). Degree certificate authentication using QR code and smartphone. International Journal of Computer Applications, 120(16).

[37] Goyal, S., Yadav, S., & Mathuria, M. (2016, September). Exploring concept of QR code and its benefits in digital education system. In 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI) (pp. 1141-1147). IEEE.

[38] Aini, Q., Rahardja, U., Tangkaw, M. R., Santoso, N. P. L., & Khoirunisa, A. (2020). Embedding a blockchain technology pattern into the QR code for an authentication certificate. Jurnal Online Informatika, 5(2), 239-244.

[39] Wellem, T., Nataliani, Y., & Iriani, A. (2022). Academic Document Authentication using Elliptic Curve Digital Signature Algorithm and QR

Code. JOIV: International Journal on Informatics Visualization, 6(3), 667-675.

[40] Khalil, G., Doss, R., & Chowdhury, M. (2019). A comparison survey study on RFID based anti-counterfeiting systems. Journal of Sensor and Actuator Networks, 8(3), 37.

[41] Kewale, P., Gardalwar, A., Vegad, P., Agrawal, R., Jaju, S., & Dabhekar, K. (2021, September). Design and implementation of RFID based e-document verification system. In 2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA) (pp. 165-170). IEEE.