The Scientific Temper (2024) Vol. 15 (spl-2): 188-195

E-ISSN: 2231-6396, ISSN: 0976-8653

Doi: 10.58414/SCIENTIFICTEMPER.2024.15.spl-2.30

https://scientifictemper.com/

RESEARCH ARTICLE

Secure degree attestation and traceability verification based on zero trust using QP-DSA and RD-ECC

Shantanu Kanade[1*], Anuradha Kanade[2]

Abstract

The process of rendering authenticity to the Degree Certificate (DC) is known as Degree Attestation (DA). None of the prevailing works have focused on zero trust-based DA, verification, and traceability for secured DA. So, zero trust-based secured DA, verification, and traceability of degree credentials are presented in the paper. Primarily, to upload the DC of the student, the university registers and logs in to the Blockchain (BC). Subsequently, by utilizing radioactive decay-based elliptic curve cryptography (RD-ECC), the DC is secured. Next, by utilizing Glorot initialization-based Proof-of-Stake (GPoS), the data is stored in the BC. Further, to verify the traceability of the data, a Smart Contract (SC) is created. In the meantime, the student registers and logs in to the BC and gives attestation requests to the university. By utilizing rail fence cipher (RFC) RD-ECC hash-based message authentication code (RFCR-HMAC), the university authenticates the request. By utilizing a quadratic probing-based digital signature algorithm (QP-DSA), the university attests the DC after authentication. Lastly, by utilizing RD-ECC, the attested certificate is encrypted and sent to the student. Hence, the certificate is secured with an encryption time (ET) of 5971ms and DA is performed with a Signature Generation Time (SGT) of 6637ms.

Keywords: Degree attestation, Blockchain, Data encryption, Smart contract, Hash-based message authentication code, Elliptic curve cryptography, Higher education credentials.

Introduction

A document provided by universities and other educational institutions to the student is the DC (Song *et al*., 2024). These DCs act as the Higher Education Credentials (HEC) for the students (Hardjono & Smith, 2021). Attestation and authenticity of the degree credentials are significant in today's digital world (Cihon *et al*., 2021). The DA and verification without tampering and unauthorized users are vital since digitalization is increasing (Zhao & Si, 2021). In addition, the establishment of trust at every stage of the attestation framework is significant (Aldwairi *et al*., 2023). This can be enhanced by the BC that securely stores the data and transacts it to the authorized student (Khan & Ahmad, 2022).

In the prevailing works, the DA via the BC has been performed. However, the security of the data utilizing Rivest-Shamir-Adleman (RSA) (Saramago *et al*., 2021) and advanced encryption standard (AES) (Sathya *et al*., 2021) in BC is prone to hacking. Numerous prevailing works utilized manual methodologies for attestation, thereby causing data breaches (Labayen *et al*., 2021). In addition, the prevailing methodologies did not consider the effective storage of the credentials (Al Hemairy *et al*., 2024) and zero trust-based DA. Thus, a new approach for secure DA and verification architecture utilizing RFCR-HMAC and QP-DSA is proposed in this paper.

Problem Statement

The prevailing works' limitations are given as follows,

- None of the existing works focused on DA, authentication, and security of DC by zero trust verification at every single stage.
- The manual DA in (Reddy *et al*., 2021) caused the tampering of degree credentials.

[1]Symbiosis School for Online and Digital Learning, Symbiosis International (Deemed) University, Pune, Maharashtra, India.

[2]MIT World Peace University, Pune, Maharashtra, India.

***Corresponding Author:** Shantanu Kanade, Symbiosis School for Online and Digital Learning, Symbiosis International (Deemed) University, Pune, Maharashtra, India, E-Mail: shantanukanade@gmail.com

How to cite this article: Kanade, S., Kanade, A. (2024). Secure degree attestation and traceability verification based on zero trust using QP-DSA and RD-ECC. The Scientific Temper, **15**(spl-2):188-195.

Doi: 10.58414/SCIENTIFICTEMPER.2024.15.spl-2.30

Source of support: Nil

Conflict of interest: The authors declare no competing interests related to Secure degree attestation and traceability verification based on zero trust using QP-DSA and RD-ECC.

© The Scientific Temper. 2024

Received: 29/10/2024 **Accepted:** 23/11/2024 **Published**: 30/11/2024

- Huge amounts of data stored in the BC were susceptible to data hacking (Khan *et al*., 2021).
- The authentication of the student's request for DA was not considered (More *et al*., 2021), thus causing a data breach.

The proposed work's contribution is explained as follows,

- The DA, verification, and traceability are performed by establishing zero trust verification of DC at every single stage.
- The digital DA is carried out with the aid of the QP-DSA technique, thus avoiding data tampering.
- To secure the DC, the RD-ECC methodology is utilized and further DC is stored in the BC by the GPoS technique.
- The RFCR-HMAC process is utilized for the authentication of the student's request.

The rest of the paper is organized as follows: The prevailing works are surveyed in Section 2, the proposed model is explained in Section 3, the performance assessment is assessed in Section 4, and the paper is concluded in Section 5 with future scope.

Literature Survey

(Reddy *et al*., 2021) established a reliable methodology to secure and verify the credentials of the students in BC. In this, the data was stored in the BC in which by utilizing secure hash algorithm 256 (SHA-256), the hash value was created. Then, for DA, the student entered the name and Aadhar details. However, the authenticity betwixt the student and the university was not checked, thereby causing a third-man attack.

(Khan *et al*., 2021) introduced a secured DA and verification framework for HEC. In this, for HEC attestation, the student gave an online request. The student sends the DC through courier after finalizing the appointment. Subsequently, the traceability was finalized via direct communication between the university and the student. But, the manual DA led to tampering with documents.

(More *et al*., 2021) developed a global authentication scheme associated with educational credentials. The documents to be attested were primarily stored in the distributed ledger. Subsequently, to provide global authentication, a SC was utilized. The credentials were approved by the verifier. Then, the credentials were sent to the specific owner. Thus, the automated DA was made. However, the system was complex and rendered high latency.

(Wabersich *et al*., 2020) Analyzed a probabilistic approach for secure DA. In this, to provide safety certificates, the Probabilistic Model Predictive Safety Certification (PMPSC) methodology was utilized. By utilizing probabilistic set invariance, the safety of the attested certificates was improved. Hence, the DA was made securely. However, the information's traceability was not checked, thus causing the tampering of DC.

(Malsa *et al*., 2021) established a BC-enabled certificate verification system. In this, the certificates were captured via a camera and stored in the BC. Subsequently, with an online request, the university attested the DC for every single student. Grounded on the solidity programming language, a SC was created. But, the certificate was not secured, which might have tampered with the DC.

Proposed Secure Degree Attestation Methodology

Figure 1 depicts the QP-DSA and RD-ECC-based secure DA approach.

University Registration and Login

Primarily, the university (R) registers into the blockchain with the university name (f_1) and university address (f_2). As described below in section 3.2, by using the RD-ECC method, a Private Key (PK) (φ) is created during the registration. After registration, (R) log into the BC to upload the DC (g) of the student utilizing the username (b_1), password (b_2), and key (φ).

Data Encryption

Initially, (g) is encrypted utilizing RD-ECC for uploading (g) into the BC securely. For data encoding, the elliptic curve cryptography (ECC), which safeguards the data from unauthorized access, is utilized. But, the random numbers utilized for PK generation might be compromised. Therefore, by utilizing the radioactive decay (RD) function, random numbers are generated. RD function generates unpredictable, unique random numbers. The data encryption process is described as,

Primarily, the (D) number of DCs can be signified as,

$$g = [g_1, g_2, g_3, ..., g_D] \tag{1}$$

Currently, (g) is secured utilizing RD-ECC, which is shown below,

Elliptic Curve

Primarily, the elliptic curve (α) is formed for protection (g). The curve (α), which has a set of points, satisfies the following mathematical formula,

$$s^2 = t^2 + (c * t) + d \tag{2}$$

Here, the variables of (α) are represented as (s,t), and the constant is specified as (c,d).

Key Generation

Subsequently, by utilizing the public key (i) and (α), the PK (A) is generated. Primarily, by utilizing (c,d) and the point (χ) of (α), (i) is generated as follows,

$$i = (c + d) * \chi \tag{3}$$

Currently, by utilizing $(i), (A)$ is generated. Grounded on the integration $(\int)$ and differentiation (∂) of the points (χ)

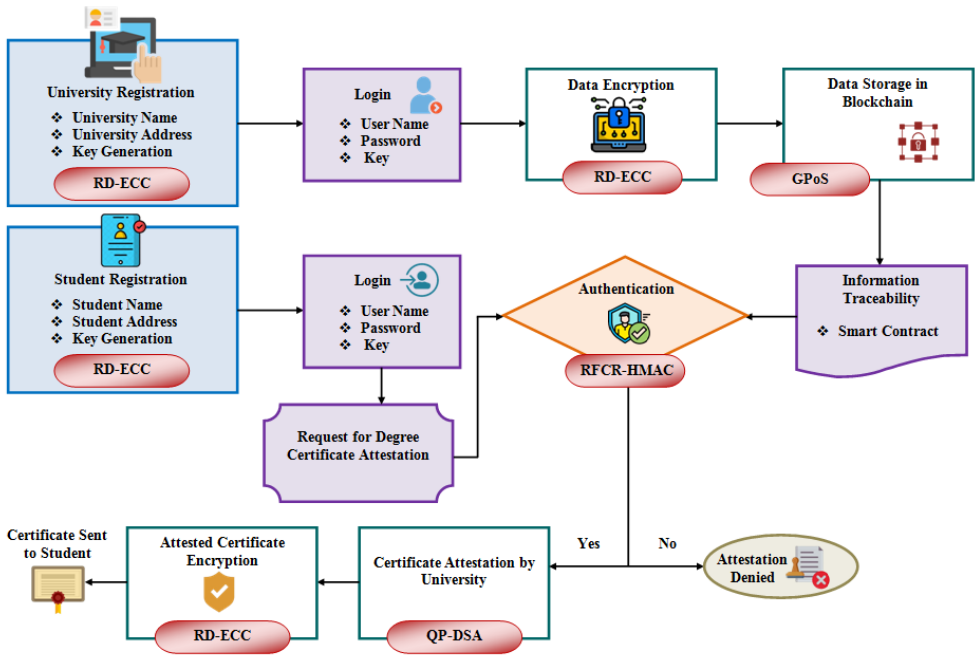


Figure 1: Framework of the proposed model

on the curve, the random number (h) is assigned by the RD function.

$$A = i \otimes h \quad \forall (A \to \beta, \phi, \Omega) \tag{4}$$

$$h = \int_{-\infty}^{\infty} \frac{\partial(\chi)}{\chi} \tag{5}$$

Here, the PK generated for the BC, university, and student are indicated as (β, ϕ, Ω).

Encryption

Lastly, with the help of (A), $(g)$is encrypted, which is shown below,

$$g^* = g \oplus A \tag{6}$$

Here, the encrypted degree certificate (data) is denoted as (g^*).

Pseudo-code for RD-ECC

Input: Degree Certificate (g)
Output: Encrypted Data (g^*)
Begin
Initialize (s,t)
Generate (α)

$$s^2 = t^2 + (c * t) + d$$

While $(\chi \in \alpha)$
Create $i = (c + d) * \chi$
Evaluate random number

$$h = \int_{-\infty}^{\infty} \frac{\partial(\chi)}{\chi}$$

Generate PK
$A = i \otimes h \quad \forall (A \to \beta, \phi, \Omega)$
For (A)
Encrypt data

$$g^* = g \oplus A$$

End for
End while
Obtain (g^*)
End

Then, the encrypted data is stored in the BC for further processing.

Data Storage

In this, by utilizing the GPoS method, (g^*) is stored in the BC. For data storage, the Proof-of-Stake (PoS) that creates new blocks is utilized. But, the stake (block) is selected randomly, thus resulting in difficulty in data storage. Thus, by using the glorot initialization technique, the block is chosen. To choose the required block, the glorot initialization technique utilizes the differentiation function. The data storage technique is explained as follows.

Primarily, the nodes (a) from the BC utilized for data storage are initialized as follows,

$$a = [a_1, a_2, a_3, ..., a_{B-1}, a_B] \tag{7}$$

Here, (B) is the number of (a). Subsequently, grounded on the Glorot initialization, the blocks (G) needed for the

storage of $(g^*)$are chosen. Glorot initialization accurately chooses the blocks among (a)as,

$$G = \sum a * \frac{\partial a}{B} \tag{8}$$

After selecting (G), the validator (q)that passes (g^*)into the blocks is generated by,

$$q = \frac{G}{a^{-1}} \tag{9}$$

Lastly, the encrypted data is stored in the BC utilizing (q) This is because, (q) at high stake verifies the transaction and passes (g^*) to the required block. After data storage, for recording and tracking the DC, the traceability of (g^*) is identified.

Traceability of Information

In this, by utilizing the SC, the traceability of (g^*) helps in giving notification to the university concerning any changes in the data stored in the BC. Primarily, the contract of the university $(R)$and the BC (J) is created as follows,

$$\delta = R + \phi \tag{10}$$
$$\varepsilon = J + \beta \tag{11}$$

Here, the individual contracts of (R) and (J) are specified as (δ, ε), and the PK of (R) and (J) created utilizing RD-ECC is denoted as (ϕ, β). For tracing the information, a SC (P) is created as follows,

$$P = \left[\delta \oplus \varepsilon\right] g^* \tag{12}$$

By utilizing (P), the traceability of (g^*) is checked continuously. Then, the student gives a request for DA, and authentication is performed.

Request for Attestation and Authentication

In this, the student (E) gives a request for DA, and then the university performs the authentication of the student's credentials (j_1, j_2), which is shown below,

Student Registration and Login

Primarily, by utilizing the student's name (j_1) and address (j_2), the student (E)registers into the BC. A PK $(\Omega)$is created for (E) utilizing the RD-ECC methodology during registration. Then, by utilizing a username (V_1), password (V_2), and (Ω), (E)log into (J) to render a DA request.

Attestation Request

After (E) login, a request (U) is sent to $(R)$for DA. The university checks (j_1, j_2) and authenticates (E).

Authentication

In this, by utilizing RFCR-HMAC, the authentication of (U) is performed. For authentication, the Hash-based Message Authentication Code (HMAC) that utilizes the keys and hash for generating unique code is used. However, the secret key generated in HMAC might be attacked, thus causing the forgery of DC. Therefore, to generate the secret key, the RFC is utilized. In addition, to improve the authentication, the PK generated utilizing the RD-ECC methodology is also utilized along with HMAC. The RFCR-HMAC methodology is explained by,

Primarily, by utilizing RFC, (j_1, j_2) is ciphered for (U). For ciphering the data, RFC utilizes the transpose function. It is equated as,

$$W = \left[U\left(j_1, j_2\right) + U\left(j_1, j_2\right)^{-1}\right] + \eta \tag{13}$$

$$\eta = W \oplus \left(\phi / \Omega\right) \tag{14}$$

Here, the ciphered request is represented as (W), and the secret key generated is signified as (η). Currently, by utilizing (W), (η), the university's name (f_1), and address (f_2), the authentication code (k) is created.

$$k_1 = W \oplus \eta(\phi) \oplus \left(f_1, f_2\right) \tag{15}$$

$$k_2 = W \oplus \eta(\Omega) \oplus \left(f_1, f_2\right) \tag{16}$$

Here, the (k) created for the university is represented as (k_1) , and the code created for the student is signified as (k_2). Currently, the similarity betwixt $(k_1)$and $(k_2)$are checked for authentication (S) by,

$$S = \begin{cases} S^1 & \forall\left(k_1 = k_2\right) \\ S^2 & \forall\left(k_1 \neq k_2\right) \end{cases} \tag{17}$$

The condition specifies that if (k) is matched, then the authentication is verified (S^1), and the university further attests to the document. Also, if $(k)$is not equal, then the authentication is not verified (S^2), and the request is denied (y).

Pseudo-code for RFCR-HMAC
Input: Request (U)
Output: Authentication (S)
Begin
Initialize (ϕ, Ω)
Cipher (U)
$W = \left[U\left(j_1, j_2\right) + U\left(j_1, j_2\right)^{-1}\right] + \eta$
Create $\eta = W \oplus \left(\phi / \Omega\right)$
For (W)
Generate code
//**University**

$$k_1 = W \oplus \eta(\phi) \oplus (f_1, f_2)$$

//**Student**

$$k_2 = W \oplus \eta(\Omega) \oplus (f_1, f_2)$$

Check similarity

If $(k_1 = k_2)$

(S^1)

Else

(S^2)

End if

End for

Return (S)

End

Subsequently, for the authenticated request, the DA is performed.

Certificate Attestation by University

Now, by utilizing QP-DSA, the DA is performed for (S^1) by the university. For DA, the Digital Signature Algorithm (DSA) that generates the digital signature quickly is utilized. However, the hash utilized by DSA could be hacked and cause information loss. Thus, for creating the hash, the Quadratic Probing (QP) function, which resolves the hash collision by adding arbitrary quadratic polynomials, is utilized. In Figure 2, the process of DA is given.

Initially, (g^*) is decrypted by (A) for obtaining the original DC (g) as,

$$g = g^* - A \tag{18}$$

Now, by utilizing a key pair that comprises the public key (i) and the hash (N), the university (R) attests (g). In this, by using the QP function, (N) is generated. For creating a unique hash, the QP function utilizes the quadratic formula.

$$N = l^2(g) + m(g) + n \tag{19}$$

Here, quadratic polynomials are indicated as (l, m, n)

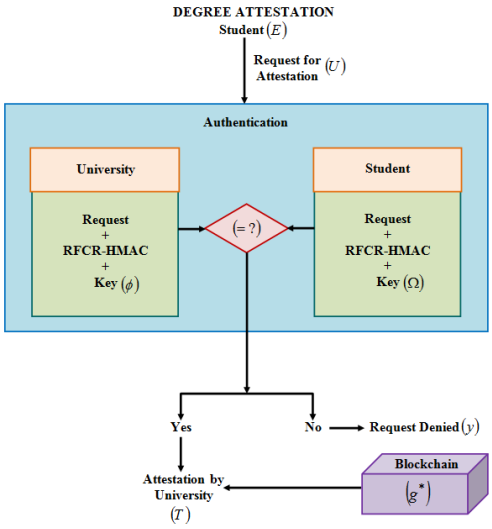


Figure 2: Degree attestation procedure

. Currently, the digital signature (T) is created in the DC as equated below,

$$T = g \oplus (i, N) \tag{20}$$

Where, the attested certificate is specified as (T). Lastly, by utilizing RD-ECC, (T) is encrypted.

Attested Certificate Encryption

In this, for encryption of (T), (A) and (i) generated using RD-ECC is used. It is articulated as follows,

$$T^* = T + A + i \tag{21}$$

Here, (T^*) is the encrypted (T). Lastly, (T^*) is sent to the student, the decryption of (T^*) occurs on the student side, and (T) gets downloaded by the student. Thus, for secured DA, the DA, verification, and validation are performed. The proposed work's performance is provided as follows,

Results And Discussion

Here, to assess the performance of the proposed model, the proposed technique is contrasted with the conventional techniques. The entire work is implemented in the PYTHON platform.

Performance Analysis of the Proposed Work

In this section, the performance of the proposed QP-DSA, RFCR-HMAC, RD-ECC, and GPoS by contrasting them with related techniques is explained. Figure 3 illustrates the performance evaluation of the proposed QP-DSA,

The SGT and signature verification time (SVT) of the proposed QP-DSA with traditional DSA, Schnorr signature (SS), RSA, and ElGamal techniques are contrasted in Figure 3. By mitigating hash function vulnerabilities in DSA, QP improves security. This ensures effective digital signature operations by attaining the minimum SGT and SVT of 6637ms and 7391ms, respectively. However, maximum average SGT and SVT of 8878ms and 9711ms, correspondingly,

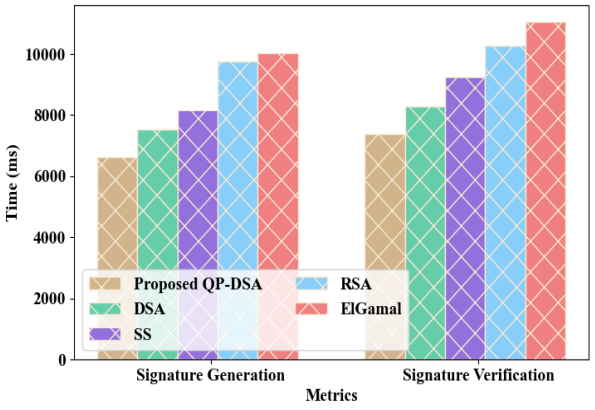


Figure 3: Signature Generation and Signature Verification Times

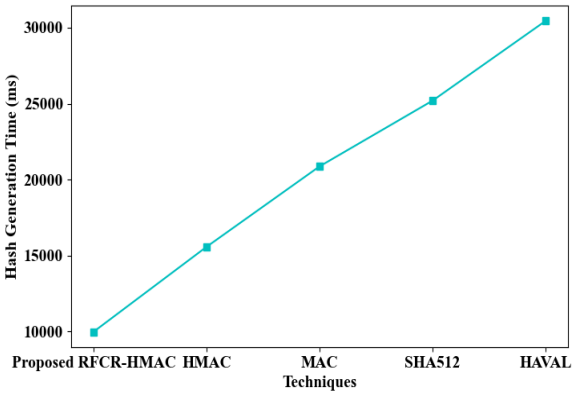


Figure 4: Comparative analysis based on hash generation time

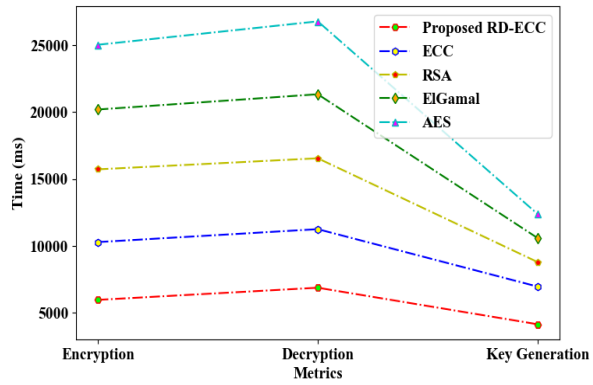
were achieved by the conventional techniques, thereby degrading the overall performance.

As illustrated in Graph 4 and Table 1, the focus on minimum hash generation time (HGT) and high entropy may affect the effectiveness of the work in prevailing HMAC, message authentication code (MAC), secure hash algorithm-512 (SHA512), and HAVAL. However, by safeguarding the secret key with RFCR, augmenting entropy, and minimizing HGT for efficient authentication, the proposed HMAC improves security. In the meantime, a minimum HGT of 9981ms and a high entropy value of 29.71 were achieved by the proposed framework. So, the proposed work ensures robust protection against forgery and unauthorized access when contrasted with the prevailing techniques.

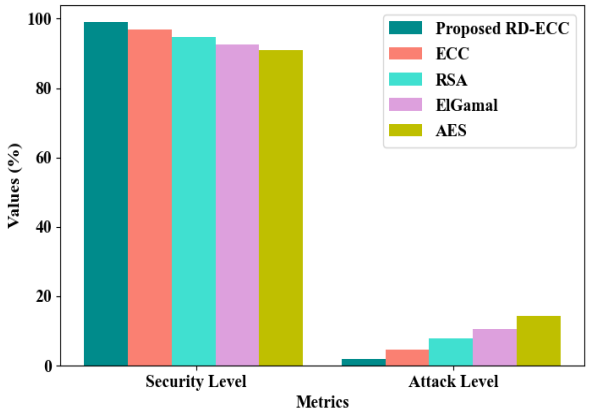
The performance evaluation of the proposed RD-ECC with the conventional ECC, RSA, ElGamal, and AES techniques is shown in Figures 5 (a), (b), and (c). In this, the proposed work improves key security by generating unpredictable random numbers via RD by mitigating vulnerabilities and also ensuring robust protection against data attacks, thereby improving performance. Hence, minimum encryption, decryption, and key generation times of 5971, 6878, and 4148 ms, correspondingly, were achieved by the proposed RD-ECC with a minimum memory usage of 1587465891kb (encryption) and 2246105673kb (decryption). However, as illustrated in graphs 5 (a) and (c), the existing methodologies used maximum time with maximum memory usage. In addition, the proposed RD-ECC secured the DCs with a high-security level (SL) of 98.95%, whereas the conventional

Table 1: Entropy of the proposed RFCR-HMAC

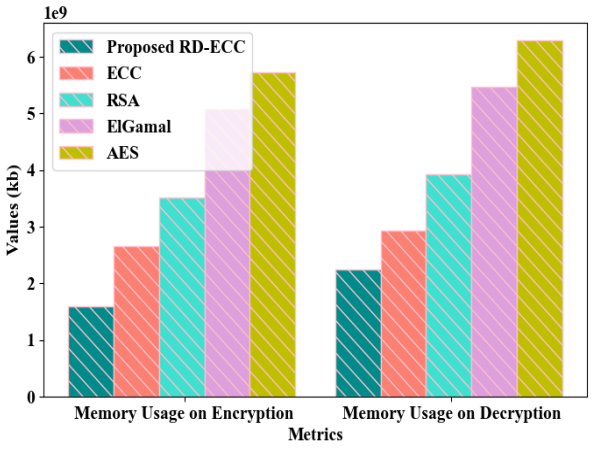
Techniques	*Entropy*
Proposed RFCR-HMAC	29.71
HMAC	26.93
MAC	23.57
SHA512	20.45
HAVAL	17.96



(a)



(b)



(c)

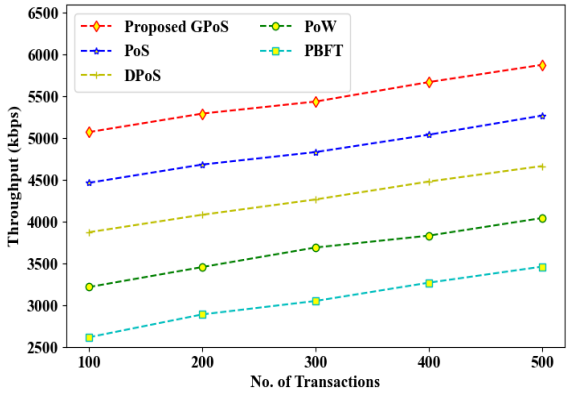
Figure 5: (a) Encryption, decryption, key generation time (b) Security and attack level (c) Memory usage on encryption and decryption for the proposed RD-ECC

Table 2: Average energy consumption

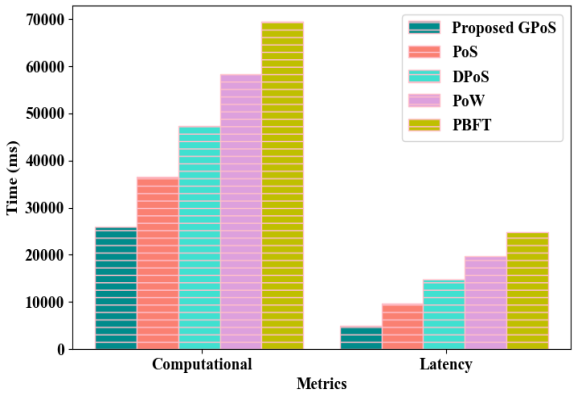
Techniques	*Average energy consumption (J)*
Proposed GpoS	22.57
PoS	26.83
DpoS	30.91
PoW	34.58
PBFT	38.79

Table 3: Comparative analysis with existing works

Study	*Techniques used*	*Security Level*	*Drawbacks*
Proposed work	RD-ECC	98.95%	-
(Shaikh *et al*., 2022)	SHA-256	-	Scalability issues
(Fekete & Kiss, 2023)	GDPR	89	Increased attack level
(Harer & Fill, 2022)	IPFS	95	Maximum latency
(Kistaubayev *et al*., 2023)	EBC	-	Potential scalability issues.
(Khurshid & Raza, 2023)	TOCTOU	-	Lacks support for low-powered devices.



(a)



(b)

Figure 6: (a) Throughput analysis (b) Computational time and latency for the proposed GpoS

ECC, RSA, ElGamal, and AES secured the DCs with a low SL of 96.87, 94.81, 92.63, and 90.94%, respectively. The proposed RD-ECC achieved a low attack level of 1.87% despite high security, whereas a high attack level of 4.59, 7.72, 10.57, and 14.39% were obtained by the prevailing techniques. Hence, data integrity and confidentiality can be compromised by this high attack level. On the contrary, superior performance is ensured by RD-ECC, which is thus established as a robust cryptographic solution to safeguard sensitive data.

Figures 6 (a) and (b) and Table 2 describe throughput analysis (TA), computational time (CT), latency, and average energy consumption (AEC) of the proposed GpoS and the existing PoS, delegated proof of stake (DpoS), proof of work (PoW), and practical byzantine fault tolerance (PBFT). The conventional work has maximum average AEC, CT, and latency of 32.77J, 52882, and 17220 ms with a minimum throughput of 4467, 3875, 3219 and 2618 kbps for 100 transactions, whereas the proposed GpoS have a minimum AEC of 22.57J with minimum CT and latency of 25891ms and 4981ms, correspondingly, as displayed in graph 6 and table 2. In addition, the proposed GpoS has a maximum throughput of 5074kbps, 5295kbps, 5439kbps, 5672kbps, and 5879kbps for 100 transactions, 200 transactions, 300 transactions, 400 transactions, and 500 transactions, correspondingly. By efficiently selecting stakes (blocks) via a methodologically informed framework, glorot initialization in the proposed PoS improved data storage accuracy. Thus, for enhanced transaction processing and block creation, glorot initialization optimizes the PoS consensus mechanism. Hence, the glorot initialization improved the proposed technique's overall performance when analogized with prevailing techniques.

The proposed and traditional works are compared in Table 3. As shown in Table 3, techniques, namely SHA-256, general data protection regulation (GDPR), interplanetary file system (IPFS), Ethereum blockchain consortium (EBC), and time-of-check to time-of-use (TOCTOU) were utilized by conventional works, whereas the proposed work utilized RD-ECC technique. In this, a low SL of 89 and 95% was achieved by the prevailing GDPR and IPFS techniques, whereas the proposed work obtained a higher SL of 98.95%. By generating unpredictable random numbers, the usage of RD in the proposed ECC improved the model, whereas the existing techniques had drawbacks, such as complexity, scalability issues, increased attack level, latency owing to BC confirmation, high transaction costs, dependency concerns, and lack of support for low-powered devices, thus degrading the overall performance of top-notch techniques. Thus, the proposed work performed better than the conventional techniques in securing the DCs.

Conclusion

By utilizing QP-DSA and RD-ECC, this research secured DA and verified traceability correspondingly. The work began with the registration and login of the university into the BC.

In this, by utilizing RD-ECC, the key was generated during registration with a duration of 4148 ms. Next, the DCs% were secured with a high SL and an attack level of 98.95% and 1.87, respectively. Subsequently, by utilizing GPoS, encrypted DC was stored with CT and AEC of 25891 ms and 22.57 J, correspondingly. Then, by using SC, the traceability was verified. In the meantime, the student logged in to the BC and gave a request for DA. Currently, by utilizing RFCR-HMAC, the university authenticated the request with an HGT of 9981 ms. Lastly, by utilizing QP-DSA, DA was performed for the authenticated request by the university with an SGT of 6637ms. Hence, the DA certificate was encrypted and sent to the students. Thus, DA was efficiently secured by the proposed model.

Future Recommendation

By utilizing several techniques, DA was efficiently secured by the proposed work. But, the students did not verify the credentials issued by the university. Thus, the DC tampering will be checked by the students in the future to enhance the efficacy of DA security.

References

Al Hemairy, M., Talib, M. A., Khalil, A., Zulfiqar, A., & Mohamed, T. (2024). Blockchain-based framework and platform for validation, authentication & equivalency of academic certification and institution's accreditation: UAE case study and system performance (2022). *Education and Information Technologies*, 1–30. https://doi.org/10.1007/s10639-024-12493-6

Aldwairi, M., Badra, M., & Borghol, R. (2023). DocCert: Nostrification, Document Verification and Authenticity Blockchain Solution. *5th International Conference on Blockchain Computing and Applications*, 652–657. https://doi.org/10.1109/BCCA58897.2023.10338908

Cihon, P., Kleinaltenkamp, M. J., Schuett, J., & Baum, S. D. (2021). AI Certification: Advancing Ethical Practice by Reducing Information Asymmetries. *IEEE Transactions on Technology and Society*, *2*(4), 200–209. https://doi.org/10.1109/tts.2021.3077595

Fekete, D. L., & Kiss, A. (2023). Toward Building Smart Contract-Based Higher Education Systems Using Zero-Knowledge Ethereum Virtual Machine. *Electronics (Switzerland)*, *12*(3), 1–39. https://doi.org/10.3390/electronics12030664

Hardjono, T., & Smith, N. (2021). Towards an attestation architecture for blockchain networks. *World Wide Web*, *24*(5), 1587–1615. https://doi.org/10.1007/s11280-021-00869-4

Harer, F., & Fill, H. G. (2022). Decentralized Attestation and Distribution of Information Using Blockchains and Multi-Protocol Storage. *IEEE Access*, *10*, 18035–18054. https://doi.org/10.1109/ACCESS.2022.3150356

Khan, A. 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 (Switzerland)*, *11*(22), 1–22. https://doi.org/10.3390/app112210917

Khan, A. U. R., & Ahmad, R. W. (2022). Blockchain-based Academic Degrees Issuance and Attestation. *International Conference on IT and Industrial Technologies*, 1–5. https://doi.org/10.1109/ICIT56493.2022.9989203

Khurshid, A., & Raza, S. (2023). AutoCert: Automated TOCTOU-secure digital certification for IoT with combined authentication and assurance. *Computers and Security*, *124*, 1–11. https://doi.org/10.1016/j.cose.2022.102952

Kistaubayev, Y., Mutanov, G., Mansurova, M., Saxenbayeva, Z., & Shakan, Y. (2023). Ethereum-Based Information System for Digital Higher Education Registry and Verification of Student Achievement Documents. *Future Internet*, *15*(1), 1–19. https://doi.org/10.3390/fi15010003

Labayen, M., Vea, R., Florez, J., Aginako, N., & Sierra, B. (2021). Online Student Authentication and Proctoring System Based on Multimodal Biometrics Technology. *IEEE Access*, *9*, 72398–72411. https://doi.org/10.1109/ACCESS.2021.3079375

Malsa, N., Vyas, V., Gautam, J., Shaw, R. N., & Ghosh, A. (2021). Framework and smart contract for blockchain enabled certificate verification system using robotics. *Studies in Computational Intelligence*, *960*, 125–138. https://doi.org/10.1007/978-981-16-0598-7_10

More, S., Grassberger, P., Horandner, F., Abraham, A., & Klausner, L. D. (2021). Trust Me If You Can: Trusted Transformation Between (JSON) Schemas to Support Global Authentication of Education Credentials. *IFIP Advances in Information and Communication Technology*, *625*, 1–16. https://doi.org/10.1007/978-3-030-78120-0_2

Reddy, T. R., Reddy, P. V. G. D. P., Srinivas, R., Raghavendran, C. V., Lalitha, R. V. S., & Annapurna, B. (2021). Proposing a reliable method of securing and verifying the credentials of graduates through blockchain. *Eurasip Journal on Information Security*, *2021*(1), 1–9. https://doi.org/10.1186/s13635-021-00122-5

Saramago, R. Q., Jehl, L., Meling, H., & Estrada-Galinanes, V. (2021). A Tree-based Construction for Verifiable Diplomas with Issuer Transparency. *3rd IEEE International Conference on Decentralized Applications and Infrastructures*, 101–110. https://doi.org/10.1109/DAPPS52256.2021.00017

Sathya, A. R., Panda, S. K., & Hanumanthakari, S. (2021). Enabling smart education system using blockchain technology. *Intelligent Systems Reference Library*, *203*, 169–177. https://doi.org/10.1007/978-3-030-69395-4_10

Shaikh, Z. A., Khan, A. A., Baitenova, L., Zambinova, G., Yegina, N., Ivolgina, N., Laghari, A. A., & Barykin, S. E. (2022). A Blockchain Hyperledger and Non-Linear Machine Learning: A Novel and Secure Educational Accreditation Registration and Distributed Ledger Preservation Architecture. *Applied Sciences (Switzerland)*, *12*(5), 1–20. https://doi.org/10.3390/app12052534

Song, H. jin, Kim, T., Hwang, Y. W., Seo, D., & Lee, I. Y. (2024). A study on dynamic group signature scheme with threshold traceability for blockchain. *High-Confidence Computing*, *4*(2), 1–9. https://doi.org/10.1016/j.hcc.2023.100163

Wabersich, K. P., Hewing, L., Carron, A., & Zeilinger, M. N. (2020). Probabilistic model predictive safety certification for learning-based control. *IFAC-PapersOnLine*, *53*(2), 1–13. https://doi.org/10.1016/j.ifacol.2020.12.1205

Zhao, X., & Si, Y. W. (2021). NFTCert: NFT-Based Certificates with Online Payment Gateway. *IEEE International Conference on Blockchain*, 538–543. https://doi.org/10.1109/Blockchain53845.2021.00081