Available online at
https://jcrinn.com/
https://crinn.conferencehunter.com/

Journal of Computing Research and Innovation 10(1) 2025

Journal of Computing Research and Innovation

e-ISSN : 2600-8793

Digital Certificate-Based Authentication Model for Enhanced Smartphone Security

A. H. Azni[1]*, Sakiinah Altaf Hussain[2], Najwa Hayaati Mohd Alwi[3]

[1,2,3]*Faculty of Science and Technology, Universiti Sains Islam Malaysia, Bandar Baru Nilai, 71800 Nilai, N.Sembilan*
[2]*Cybersecurity and Systems (CSS) Research Unit, Faculty of Science and Technology, Universiti Sains Islam Malaysia, Bandar Baru Nilai, 71800 Nilai, N.Sembilan*

ARTICLE INFO

Article history:
Received 24 October 2024
Revised 31 December 2024
Accepted 10 January 2025
Online first
Published 1 March 2025

Keywords:
Smartphone Security
Digital Certificates
User-Device Authentication
RSA

DOI:
10.24191/jcrinn.v10i2

ABSTRACT

Smartphones are integral to the Internet of Things, facilitating connectivity for various devices such as home systems and healthcare tools. However, the growing threat of identity theft, data breaches, and attacks due to weak authentication and poor password management emphasizes the critical need for mobile device security. Cryptography is pivotal in ensuring that only authorized devices can access data. This paper introduces an innovative authentication model for smartphones, integrating digital certificates and secret keys to securely encrypt and decrypt data. The model employs the RSA algorithm to generate encryption keys and authenticate user and device identities. Aimed at addressing smartphone users' authentication needs, the model operates through three phases: Registration, Digital Certificate, and Authentication, each bolstering data protection through digital certificate-based authentication. To assess the model, expert reviews are conducted to ensure its effectiveness. The results demonstrate significant improvements in security and ease of implementation compared to traditional authentication methods. Expert reviews agree that the model effectively mitigates unauthorized access risks by strengthening encryption and authentication protocols across its three key phases. These enhancements make it particularly suited for addressing the evolving security challenges of mobile applications, setting a benchmark for future authentication frameworks in smartphone ecosystems.

1. INTRODUCTION

The rise of smartphones has revolutionized industries like healthcare, education, and technology, turning them into essential tools for daily operations and driving innovation. Their impact is evident as traditional manual processes are replaced by digital methods such as online forms and digital banking, changing how individuals and businesses operate. However, this widespread use raises serious concerns about privacy

[1]* Corresponding author. *E-mail address*: ahazni@usim.edu.my

https://dx.doi.org/10.24191/jcrinn.v10i1.496

and security. Smartphones are prone to loss, theft, and unauthorized access, which can lead to sensitive information falling into the wrong hands (Badr, Y et al., 2021). Unlike past practices where data was stored in controlled environments, the growing reliance on smartphones increases the need for advanced security measures to protect confidential data (Bahaddad et al., 2022). As smartphones store vast amounts of personal data, securing this information is critical. Information security plays a key role in protecting data integrity and privacy, particularly as users rely on smartphones for banking, communication, and online transactions. Robust security measures, such as cryptography, are essential in mitigating these threats and ensuring data protection (Pandey & Bhushan, 2024).

Cryptography is fundamental to smartphone security, offering confidentiality, integrity, and authentication. It secures personal data, communications, and transactions through methods like device encryption and biometric authentication. Techniques like the RSA algorithm and digital signatures further enhance security by verifying the authenticity of transactions and documents (Im et al., 2020; Baqeel & Saeed, 2019). This paper aims to develop a strong user-device authentication model for smartphones using digital certificates and cryptographic techniques, especially focusing on the RSA algorithm. The model is designed to provide enhanced protection against unauthorized access through a multi-phase authentication process. The paper explores existing research, the methodology of the model, and its effectiveness through expert reviews, concluding with suggestions for future smartphone security improvements.

2. RELATED WORKS

In a recent study conducted by Yaswanth and Reddy (2023), a novel authentication model was suggested to enhance security in smartphone applications. The model leverages the RSA algorithm to generate a transaction password and incorporates a time-based one-time password (OTP) along with a PIN during the cryptographic key generation phase. The encrypted OTP is transmitted to the server within a specified time frame to facilitate secure key exchange between the client and server, rendering any message alteration ineffective. While robust in terms of confidentiality and security compliance, this approach may lead to a complex user experience due to the frequent generation of OTPs and remains susceptible to phishing attacks. Additionally, it remains susceptible to phishing attacks, wherein malicious actors could exploit users to reveal their OTPs. While RSA ensures strong security with large key sizes, its computational intensity is limited, especially on mobile devices. In contrast, Elliptic Curve Cryptography (ECC), offering similar security with significantly smaller key sizes, presents a more efficient solution in resource-constrained environments such as smartphones.

A biometric authentication model using digital signatures was introduced to enhance data security. Oudah and Maolood (2022) proposed a combination of the Elliptic Curve Digital Signature Algorithm (ECDSA) with Secure Socket Layer (SSL), creating a hybrid system that reduces computational complexity and communication overhead while maintaining high security. Users register with IoT devices, and their information is verified before an authentication certificate is issued. Although the model strengthens protection against common vulnerabilities, it mainly addresses user authentication, leaving some risk of phishing attacks through stolen device keys. Similarly, Pangan et al. (2022) proposed a model using RSA cryptography for secure online data transfer. It employs a key pair for encryption and decryption, ensuring unidirectional communication. The framework, implemented in the VacciFied system, uses a QR code and public key to encrypt sensitive data, which only the private key can decrypt. While this method prevents unauthorized access, the reliance on QR codes makes it susceptible to phishing attacks.

Furthermore, Iyanda and Fasasi (2022) explored the use of a dynamic one-time password (OTP) authentication system via SMS gateway. The OTP, generated using a PHP function, is sent to the user's mobile device through a bulk SMS provider. This two-factor authentication (2FA) combines a user-created static password with a dynamic OTP that expires after use, enhancing security. However, the need to

https://doi.org/10.24191/jcrinn.v10i1.496

repeatedly enter OTPs within a short time can reduce user convenience, and phishing risks remain, as attackers may intercept OTPs.

Lastly, Ali et al. (2021) developed a multi-factor authentication system for mobile money, integrating PIN, OTP, and biometric fingerprint verification for secure transactions. Despite increased security, the fingerprint recognition method faces concerns over spoofing and usability for users with physical limitations. Moreover, the risk of full mobile device access compromising sensitive data, like OTPs, still exists. Nevertheless, multi-factor authentication strengthens security beyond single-factor methods.

3. METHODOLOGY: PROPOSED DESIGN MODEL

A robust authentication model has been proposed to meet the increasing demand for secure mobile authentication, leveraging digital certificates to ensure user and device authenticity through advanced cryptographic techniques. The Digital Certificate-Based Authentication Model has been specifically designed for smartphone users, utilizing digital certificates to authenticate both the user and the device. The process involves identifying the requirements and scope of the authentication model for smartphone users, followed by proposing an authentication model based on user and device authentication using digital certificates. The design of this model incorporates the RSA algorithm and Digital Signature to ensure robust digital signature-based authentication for both users and devices (Ab Halim et al., 2024).

3.1 Digital Certificate-Based Authentication Model

The Digital Certificate-Based Authentication Model for smartphone users involves three phases, starting with the registration of the user and device, as shown in Fig. 1. During this phase, the user submits their ID and password, while the device registers its phone number and IMEI number. This information is stored in the control server, which generates public and private keys for both the user and the device. These keys are securely maintained by the control server. After registration, the user and device request their Digital Certificates, which are created by a third-party Certificate Authority. The Certificate Authority retrieves the required data from the control server to generate the certificates.

After the certification authority successfully creates and stores digital certificates, the subsequent login process requires sequential authentication of both the user and the device. The user needs to input their user ID and password, while the device requires the input of their phone number and IMEI number. Authentication calculations involve verifying the user and the device by comparing their public keys and digital signatures obtained from the control server and the certificate authority. Successful login depends on the joint authentication of both the user and the device. The following section will detail the three-phase process integral to the model.

https://doi.org/10.24191/jcrinn.v10i1.496

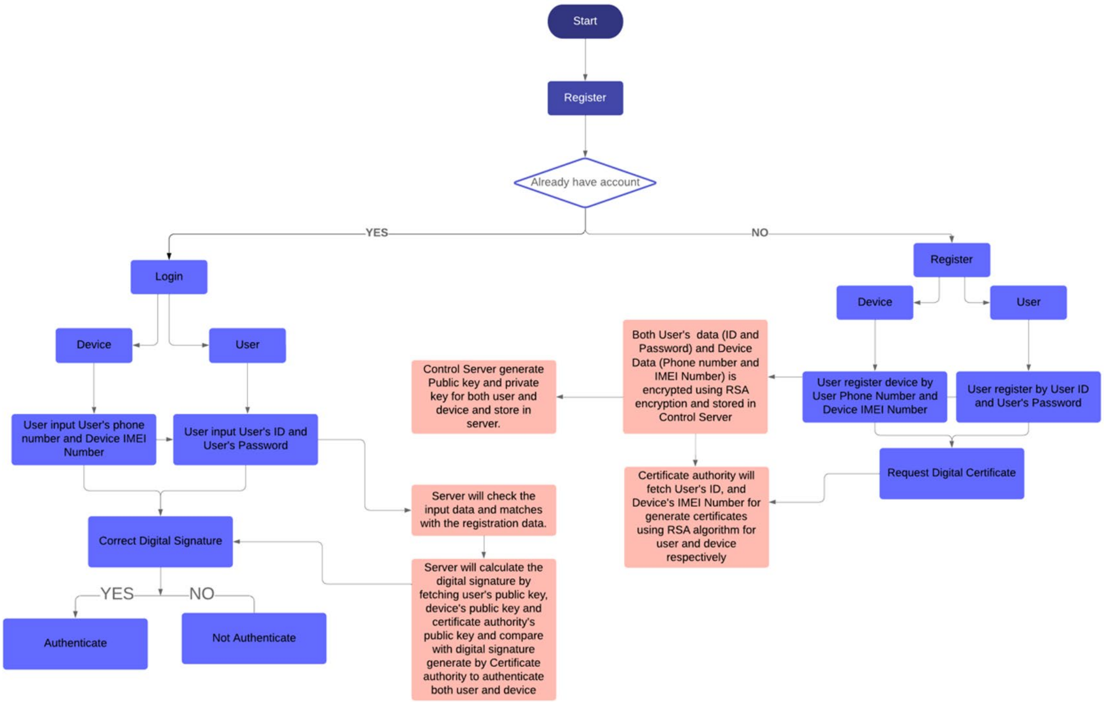

Start
Register
Already have account
YES
NO
Login
Device
User
User input User's phone number and Device IMEI Number
User input User's ID and User's Password
Correct Digital Signature
YES
NO
Authenticate
Not Authenticate
Server will check the input data and matches with the registration data.
Server will calculate the digital signature by fetching user's public key, device's public key and certificate authority's public key and compare with digital signature generate by Certificate authority to authenticate both user and device
Control Server generate Public key and private key for both user and device and store in server.
Both User's data (ID and Password) and Device Data (Phone number and IMEI Number) is encrypted using RSA encryption and stored in Control Server
Certificate authority will fetch User's ID, and Device's IMEI Number for generate certificates using RSA algorithm for user and device respectively
Register
Device
User
User register device by User Phone Number and Device IMEI Number
User register by User ID and User's Password
Request Digital Certificate

Fig. 1. Flowchart of the digital certificate-based authentication model

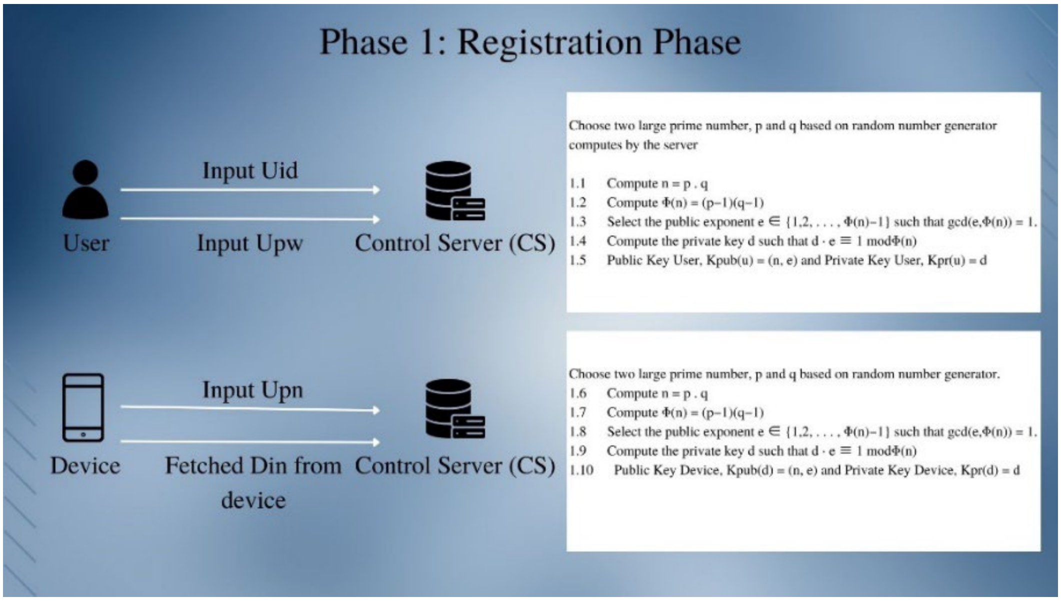
3.1.1. Phase 1: Registration Phase

The Digital Certificate-Based Authentication Model for Phase 1 involves the registration of users and their devices. During this stage, users provide their User Identity (U_{id}) and set a corresponding password (U_{pw}), which are securely stored on the control server (CS). Additionally, users register their devices by obtaining the International Mobile Equipment Identity (IMEI) number (D_{in}) and entering their phone number (U_{pn}), which are also stored on the CS.

The CS uses a random number generator to generate two large prime numbers, p and q, which are used to compute the user's cryptographic key. The value n is calculated by multiplying p and q as described in Step 1.1 in Fig. 2. This approach ensures the secure generation of cryptographic keys for user authentication. Once the value n is obtained, the next step is to calculate the Euler's Totient with the formula shown in Step 1. 2. The equation Euler's Totient above is used to calculate the public exponential, e. Public exponential, e, is selected by $e \in \{1,2, . . ., \Phi(n)-1\}$ such that $gcd(e,\Phi(n)) = 1$. The private key d is calculated based on Step 1.3. The private key user is depicted as $Kpr(u) = d$. Once the user has obtained the private key, the public key of the user is calculated using Step 1.4.

The procedure is repeated to obtain the Public Key and Private Key for the device, which are represented as $Kpub(d)$ and $Kpr(d)$, respectively. ASCII encoding is used to convert the U_{id} and D_{in} into their respective ASCII values. After that, the value is encrypted using the User's Public Key, $Kpub(u)$, along with the U_{id} and the Device's Public Key, $Kpub(d)$, for D_{in}.

https://doi.org/10.24191/jcrinn.v10i1.496



Choose two large prime number, p and q based on random number generator computes by the server

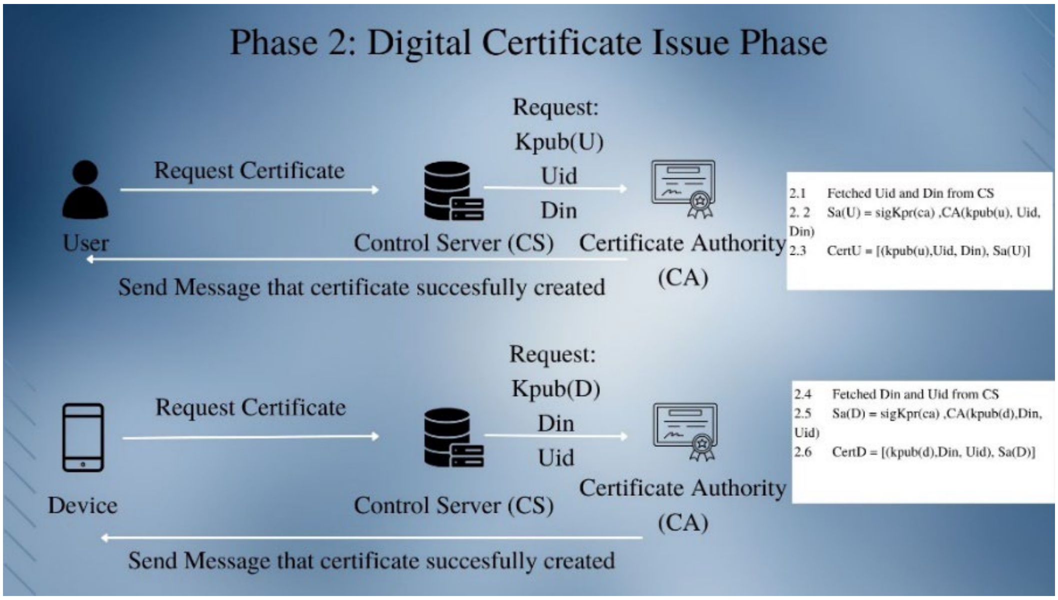
1.1 Compute n = p . q
1.2 Compute Φ(n) = (p−1)(q−1)
1.3 Select the public exponent e ∈ {1,2, . . . , Φ(n)−1} such that gcd(e,Φ(n)) = 1.
1.4 Compute the private key d such that d · e ≡ 1 modΦ(n)
1.5 Public Key User, Kpub(u) = (n, e) and Private Key User, Kpr(u) = d

Choose two large prime number, p and q based on random number generator.
1.6 Compute n = p . q
1.7 Compute Φ(n) = (p−1)(q−1)
1.8 Select the public exponent e ∈ {1,2, . . . , Φ(n)−1} such that gcd(e,Φ(n)) = 1.
1.9 Compute the private key d such that d · e ≡ 1 modΦ(n)
1.10 Public Key Device, Kpub(d) = (n, e) and Private Key Device, Kpr(d) = d

Fig. 2. Phase 1: Registration Phase

3.1.2. *Digital Certificate Issue Phase*

The process flow of the proposed Digital Certificate-Based Authentication Model for Phase 2, with a particular emphasis on the digital certificate issuance phase, is shown in Fig. 3 below. In this stage, users have to request digital certificates for their devices and themselves. The control server (CS) provides the Certificate Authority (CA), which is in charge of issuing these certificates, with the user's public key *(Kpub(u))*, user *ID* (U_{id}), and device IMEI number (D_{in}) as shown in Step 2.1.


Phase 2: Digital Certificate Issue Phase
User
Request Certificate
Control Server (CS)
Request:
Kpub(U)
Uid
Din
Certificate Authority (CA)
Send Message that certificate succesfully created
Device
Request Certificate
Control Server (CS)
Request:
Kpub(D)
Din
Uid
Certificate Authority (CA)
Send Message that certificate succesfully created

2.1 Fetched Uid and Din from CS
2. 2 Sa(U) = sigKpr(ca) ,CA(kpub(u), Uid, Din)
2.3 CertU = [(kpub(u),Uid, Din), Sa(U)]

2.4 Fetched Din and Uid from CS
2.5 Sa(D) = sigKpr(ca) ,CA(kpub(d),Din, Uid)
2.6 CertD = [(kpub(d),Din, Uid), Sa(D)]

Fig. 3. Phase 2: Digital Certificate Issues Phase

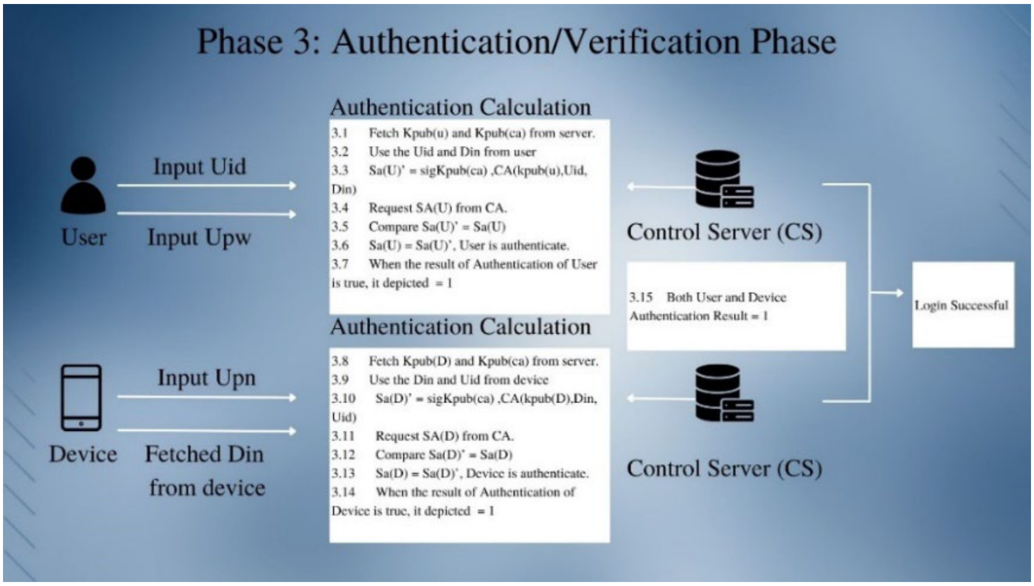
https://doi.org/10.24191/jcrinn.v10i1.496

The CA then signs the certificate with its private key *(Kpr(ca))*, which includes the user's public key, user ID, and device IMEI number. The CA keeps the user's certificate after it is issued with the information as shown in Step 2.2. The information in the certificate of the users is the user's public key, which includes the user's ID (U_{id}) and the Device's IMEI number *(*D_{in}*)*, as well as the Signature of the digital certificate; the steps below are repeated to obtain the digital certificate for the device. Once both of the certificates are created, both the user and their device receive a notification verifying the successful creation of the certificate. Each year, these certificates must be renewed to preserve the security of the user's key. The process is reiterated to procure a certificate for the user's device, with the CA signing information within the device's certificate, including the device's public key *(Kpub(d))*, device IMEI number, and user ID, using its private key *(Kpr(ca)).*

3.1.3 Authentication/Verification Phase

Phase 3, or the authentication/verification stage, is represented by the progression of the proposed Digital Certificate-Based Authentication Model in Fig. 4. The user must enter their UserID, (U_{id}), password (U_{pw}), and device's phone number (U_{pn})in this phase, which expands on Phases 1 and 2. The IMEI number of the device, D_{in} is also obtained. If the user enters U_{id}*,* U_{pw}, or U_{pn} incorrectly, an error message asks them to enter the correct information. The Control Server (CS) performs an authentication calculation to confirm the user's signature after receiving accurate input. This entails obtaining the Certificate Authority (CA) *(Kpub(ca)*) and user *(Kpub(u))* public keys from the CS. The authentication calculation uses the public key *(Kpub(ca))* of the CA to compute the user's verification signature *(Sa(U)')* based on the provided U_{id} and D_{in} (fetched from the device) as shown in Step 3.1.

The Authentication calculation then will request the value of *Sa(U)* from CA and compare them with the value of *Sa(U')*. The user is authenticated and depicted as '1' when the Control Server compares *Sa(U)* with *Sa(U)'*. This procedure is repeated for device authentication, in which the device's details and the public key of the CA are used to compute the verification signature *(Sa(D)')*. Login is made possible upon successful user and device authentication whereby both are shown as '1'. It is impossible to authenticate the user and the device together if one of them is not authenticated. The suggested Digital Certificate-Based Authentication is described in these diagrams and protocols. This proposed model will be used for expert review validation to verify the potential of this model to be adapted to smartphone users in the future.



Phase 3: Authentication/Verification Phase

User

Input Uid

Input Upw

Authentication Calculation

3.1 Fetch Kpub(u) and Kpub(ca) from server.
3.2 Use the Uid and Din from user
3.3 Sa(U)' = sigKpub(ca) ,CA(kpub(u),Uid, Din)
3.4 Request SA(U) from CA.
3.5 Compare Sa(U)' = Sa(U)
3.6 Sa(U) = Sa(U)', User is authenticate.
3.7 When the result of Authentication of User is true, it depicted = 1

Control Server (CS)

3.15 Both User and Device Authentication Result = 1

Login Successful

Device

Input Upn

Fetched Din from device

Authentication Calculation

3.8 Fetch Kpub(D) and Kpub(ca) from server.
3.9 Use the Din and Uid from device
3.10 Sa(D)' = sigKpub(ca) ,CA(kpub(D),Din, Uid)
3.11 Request SA(D) from CA.
3.12 Compare Sa(D)' = Sa(D)
3.13 Sa(D) = Sa(D)', Device is authenticate.
3.14 When the result of Authentication of Device is true, it depicted = 1

Control Server (CS)

Fig. 4. Phase 3: Authentication/Verification Phase

https://doi.org/10.24191/jcrinn.v10i1.496

4. RESULTS AND DISCUSSIONS

The paper aimed to investigate the Digital Certificate-Based Authentication Model for smartphone users and solicit expert evaluation regarding its efficacy. Experts proficient in smartphone authentication principles were engaged, and their assessments were segmented into three primary domains: registration, certificate issuance, and authentication/validation phases. The model was crafted to prioritize smartphone security, empowering users to safeguard their data and thwart unauthorized access and deceptive activities. It is anticipated to augment user experience by obviating the necessity for supplementary authentication measures. Through authenticating both the user and device, the model holds promise to enhance user experience by potentially obviating the need for recurrent authentication after the initial authorization process (Zakaria, A., et al., 2022).

4.1 Expert Review Evaluation

During the Expert Review Evaluation, a series of face-to-face and online meetings were conducted with esteemed experts to introduce the Digital Certificate-Based Authentication Model and solicit their valuable feedback. The primary aim of this assessment was to rigorously evaluate the model's suitability for practical implementation. Following a comprehensive presentation of the concept, the experts were invited to complete detailed questionnaires aimed at eliciting their insightful perspectives. The questionnaires consist of three sections and 12 questions representing every phase of the model. A total of 8 experts from academia and industry specializing in authentication actively participated in the evaluation. These distinguished experts possess extensive experience in information security, including notable contributions to academic research and significant roles in prominent technology organisation. Their discerning feedback is instrumental in refining the Digital Certificate-Based Authentication Model and ensuring its efficacy for future applications. Table 1 below details out the expert review qualification and their experiences.

Table 3. Expert review details

Name	Job Position/Expertise	Years of Experience
Expert Review 1	Senior Analyst/ Information Security	13
Expert Review 2	Senior Lecturer/ Cybersecurity, Computer Graphics	24
Expert Review 3	Software Developer	3
Expert Review 4	Cryptography Lecturer	5
Expert Review 5	Security Auditor	23
Expert Review 6	Cybersecurity Lecturer	5
Expert Review 7	IT Security Architect	27
Expert Review 8	Digital Forensics Quality Assurance and Analyst	4

4.1.1. Registration Phase Evaluation

The expert assessment of the Digital Certificate-Based Authentication Model revealed several significant findings. Below is the list of questions provided in the questionnaires for the experts to answer.

- Question 1: It is more secure to register both the user and the device rather than just registering the user for authentication on a smartphone user.
- Question 2: Registering a user's device using the user's phone number and the device's IMEI number fetched from the device is more secure for authentication compared to only registering the user's phone number.

https://doi.org/10.24191/jcrinn.v10i1.496

- Question 3: Using the Rivest–Shamir–Adleman (RSA) algorithm is suitable for generating public key and private key in smartphone user.
- Question 4: Both the user and device need to be assigned their own pair of keys by the server after registering.

The first and second questions were asked about the security of smartphones using input from both users and devices. In response to the first question, 87% of experts concurred that authenticating both the user and the device improves security by providing an additional layer of protection against unauthorized access. With regard to device registration, 75% of experts advocated for the combined use of the user's phone number and the device's IMEI to bolster authentication security and prevent device cloning. The third question suggested that the RSA algorithm be incorporated into the model, and 75% of experts concurred that it is a suitable method for generating public and private keys while acknowledging that some suggested alternative methods, such as ECC. Furthermore, all experts unanimously agreed that both the user and device should be assigned their own key pair for encryption, underscoring the critical importance of securing communications with a Certificate Authority (CA).

In addition, experts have reached a consensus that issuing two digital certificates can significantly enhance authenticity and security in smartphone applications. A substantial 63% of experts concur that this approach improves scalability and security. Furthermore, they recommend the inclusion of both the user's ID and the device's IMEI in the certificates to establish a more secure link between the user and the device. Notably, using time-limited certificates is favored, with an overwhelming 87% agreement that implementing expiration dates encourages regular updates to enhance security measures. Lastly, all experts unanimously concur that the utilization of a Certificate Authority (CA) to sign both the user and device certificates is essential for safeguarding keys from unauthorized access and ensuring robust key management practices. Fig. 5 shows the findings from Phase 1.

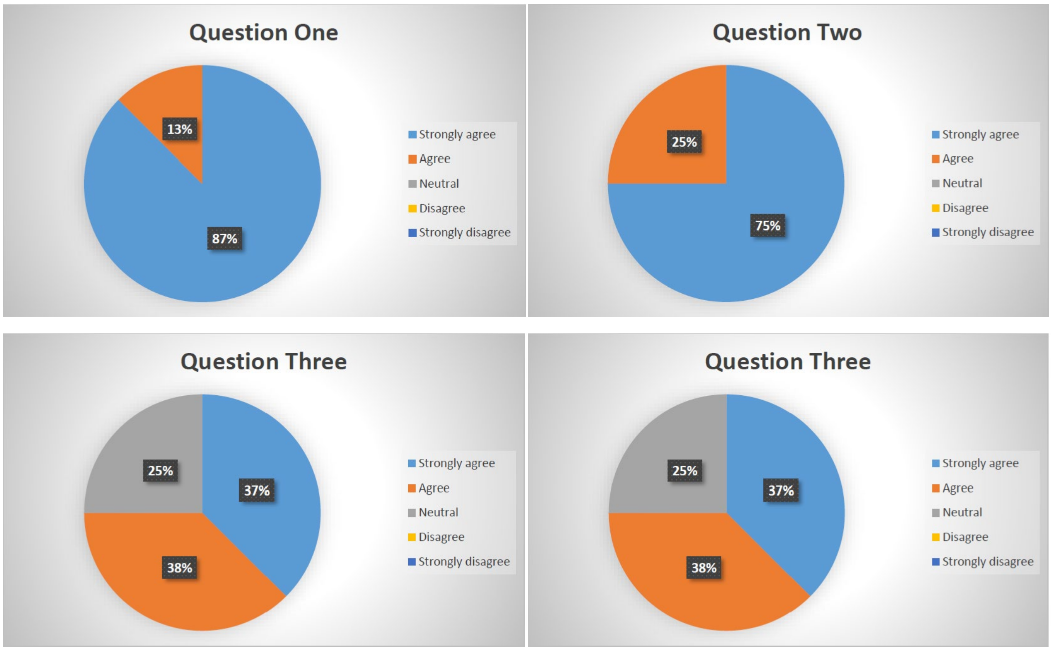


Fig. 5. Registration Phase Results

https://doi.org/10.24191/jcrinn.v10i1.496

4.1.2. Digital Certificate Issue Phase Evaluation

The Digital Certificate Issuance Phase Evaluation reveals strong support from experts for the implementation of separate digital certificates for users and devices in smartphone applications. Questions 5 until 9 below are outline a strategy for enhancing the security of smartphone applications by issuing two digital certificates.

- Question 5: Producing two digital certificates for the user and device respectively can enhance the authenticity of the user and device in smartphone applications.
- Question 6: A feasible solution to link both the user and their device is to incorporate information from both into a respective certificate (i.e: The user will have their ID and device's IMEI number in their certificate whereas the device will have their IMEI number and the user's ID in their certificate)
- Question 7: Using two digital certificates from both the user and the authentication device is better for securing smartphone applications.
- Question 8: A certificate issued by the Certificate Authority (CA) for both user and device is valid for a certain amount of time (i.e., one year). Once the certificate is no longer valid, the system will auto-request the CA to generate a new certificate.
- Question 9: Using the Certificate Authority (CA) for signing the User and Device's certificate is better to protect the key of the user and device from unauthorized access.

The approach involves incorporating user ID and device IMEI into their respective certificates, having the certificates signed by a Certificate Authority (CA), and implementing automatic renewal mechanisms to ensure continuous protection from unauthorized access. In question 5, 37% of experts strongly agree, and 63% agree, that issuing distinct certificates enhances security by allowing individual authentication for both users and devices. This approach also increases scalability and enables more granular control over system access, ensuring that only authorized devices can connect to networks or systems. Additionally, experts emphasized the importance of using unique device certificates to authenticate hardware, such as IoT devices and network equipment.

Furthermore, in questions 6 and 7, experts also agreed that linking both user and device information within certificates improves security, with 63% agreeing that this prevents attacks like Man-in-the-Middle (MITM) by validating both entities. Moreover, 87% of experts agreed that two certificates—one for the user and one for the device—provide a higher level of security for smartphone applications, especially in scenarios requiring robust authentication methods like two-factor authentication (2FA). This combination offers a stronger defense than relying on traditional methods, such as passwords or PINs.

Experts also highlighted the importance of certificate expiration for security and management. In question 8, 75% agreed that time-limited certificates promote regular key updates, reducing the risk of long-term key vulnerabilities. Finally, in question 9, 100% of experts supported using Certificate Authorities (CAs) for signing user and device certificates, agreeing that CAs enhance security by securely generating and managing keys, ensuring the protection of sensitive information against unauthorized access. Fig. 6 shows the findings from Phase 2.

https://doi.org/10.24191/jcrinn.v10i1.496

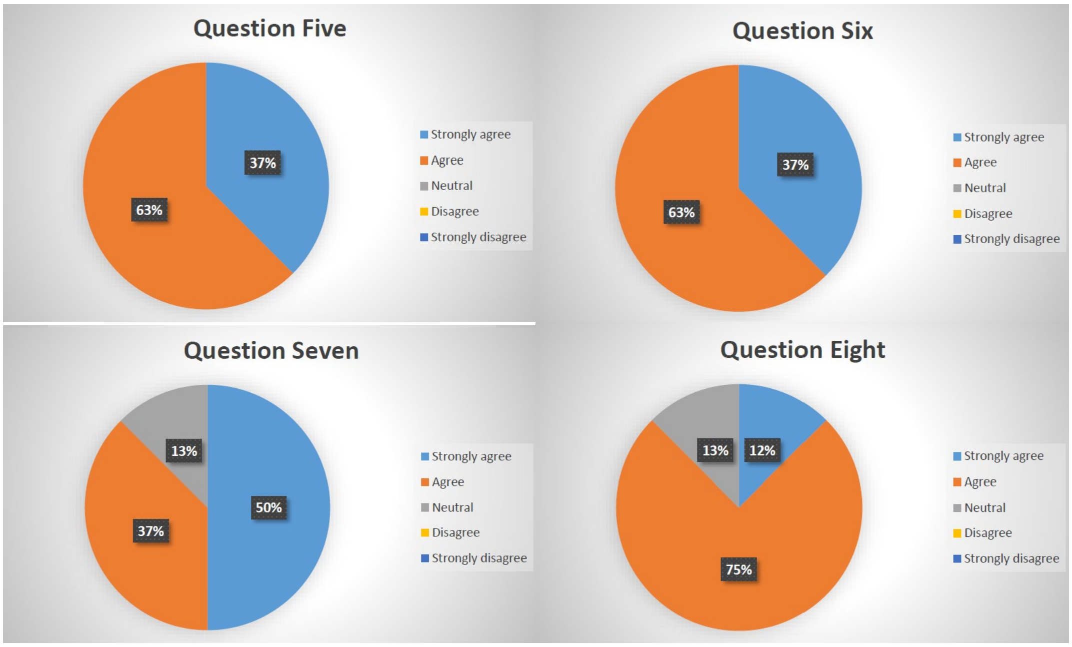


Fig. 6. Digital Certificate Issue Phase Results

4.1.3 Authenticate/Verification Phase Evaluation

The evaluation of the double authentication method using both user and device signatures in smartphone applications was asked in Question 10 until Question 12.

- Question 10: Double authentication using user and device signature is more secure compared to single authentication in smartphone applications.
- Question 11: Using Certificate Authority's Public key, Kpub(ca) to verify the signature can avoid unauthorized access in smartphone applications.
- Question 12: It is more systematic for the control server (cs) that requires the user's ID from the user and the device's IMEI number fetched from the device to calculate the signature verification separately where the authentication calculation will first calculate the signature verification from the user followed by the device.

The result shows strong support from experts. In question 10, 62% of experts strongly agreed, and 38% agreed, that this method provides a higher level of security compared to single authentication. By combining user and device signatures, this approach enhances the security of smartphone applications by confirming both the user's identity and the device's legitimacy. This reduces the chances of unauthorized access, even if an attacker obtains the user's credentials, as the device must also be authorized to complete the authentication process.

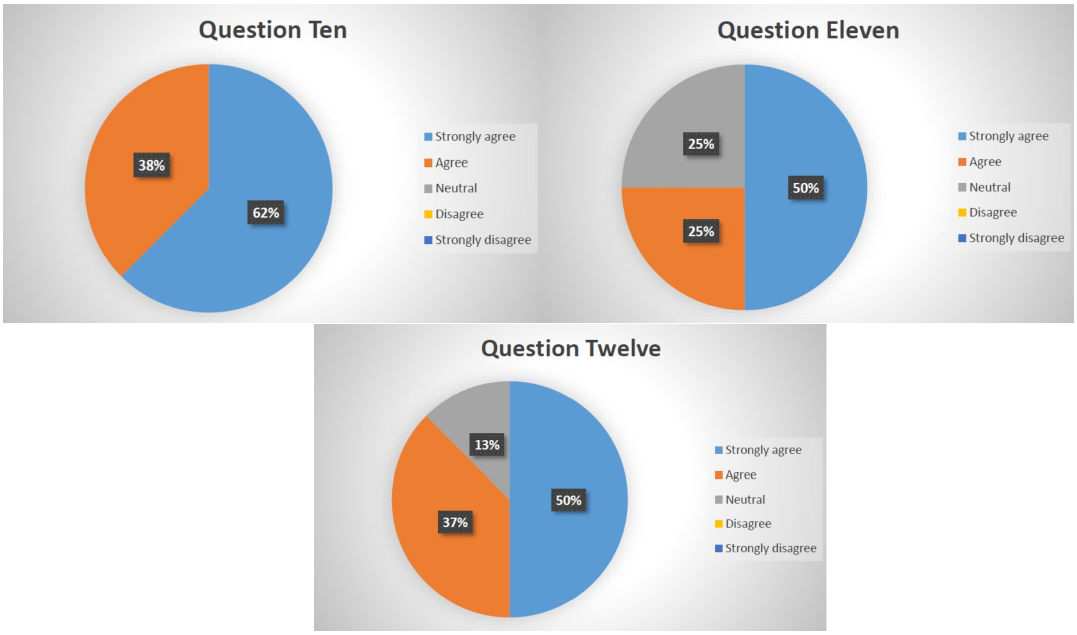


Fig. 7. Authenticate/Verification Phase Results

In question 11, 50% of experts strongly agreed, and 25% agreed, that using the Certificate Authority's public key *(Kpub(ca))* to verify digital signatures can prevent unauthorized access. This method ensures that incoming messages or authentication requests are verified with the CA-issued certificate, confirming their legitimacy. In question 12, 50% of experts strongly agreed, and 37% agreed that it is more systematic for the control server to perform separate signature verifications for the user's ID and the device's IMEI. This sequential process ensures smooth verification and confirms that both user and device signatures are legitimate before granting access. Fig. 7 shows the findings from Phase 3.

5. CONCLUSION AND RECOMMENDATIONIS

In conclusion, it is imperative to prioritize authentication for smartphone users, especially considering the rapid growth in smartphone adoption. Smartphones store extensive amounts of sensitive and personal data, such as contact details, messages, photos, and financial information. Therefore, implementing robust authentication measures is essential to safeguard user privacy and prevent unauthorized access. Strong authentication protocols ensure the security of mobile devices, protecting sensitive data from potential threats like identity theft, fraud, and breaches. Given the increasing use of smartphones for banking and payments, these security measures are particularly crucial in mitigating risks associated with financial transactions.

The three main objectives were to assess authentication requirements, create a user and device authentication model, and evaluate this model using digital certificates. However, limitations in the data collection process arose due to the complexity of the questionnaire design and the theoretical nature of the proposed model, which has not yet been tested in real-world applications. Future efforts should concentrate on practically implementing and testing the model, with potential applications across various sectors, including banking and healthcare. Furthermore, enhancing the model with hybrid cryptography methods, such as Elliptic Curve Cryptography (ECC), and integrating physical biometrics could further bolster user-device authentication in smartphones.

6. ACKNOWLEDGEMENTS/FUNDING

This research was funded by the Ministry of Higher Education (MOHE) of Malaysia under the Fundamental Research Grants Scheme (FRGS/1/2019/ICT03/USIM/02/1).

7. CONFLICT OF INTEREST STATEMENT

The authors agree that this research was conducted in the absence of any self-benefits, commercial or financial conflicts and declare the absence of conflicting interests with the funders.

8. AUTHORS' CONTRIBUTIONS

A H Azni: Conceptualisation, methodology, investigation, writing-original draft and supervision; **Sakiinah Altaf Hussain**: Conceptualisation, methodology, and formal analysis; **Najwa Hayaati Mohd Alwi**: Conceptualisation, validation, and supervision.

9. REFERENCES

Ab Halim, A. H., Ridzuan, F., Zakaria, N. H., Zakaria, A. A., Mohd Alwi, N. H., Ali Pitchay, S., Az-Zuhar, I., & AlSabhany, A. A. (2024). SAKTI©: Secured chatting tool through forward secrecy. *Journal of Advanced Research in Applied Sciences and Engineering Technology*, *49*(1), 54–62.

Ali, G., Dida, M. A., & Elikana Sam, A. (2021). A secure and efficient multi-factor authentication algorithm for mobile money applications. *Future Internet*, *13*(12), 299. https://doi.org/10.3390/fi13120299

Badr, Y., Zhu, X., & Alraja, M. N. (2021). Security and privacy in the Internet of Things: Threats and challenges. *Service Oriented Computing and Applications*, *15*(4), 257-271. https://doi.org/10.1007/s11761-021-00327-z

Bahaddad, A. A., Almarhabi, K. A., & Alghamdi, A. M. (2022). Factors affecting information security and the implementation of Bring Your Own Device (BYOD) Programmes in the Kingdom of Saudi Arabia (KSA). *Applied Sciences*, *12*(24), 12707. https://doi.org/10.3390/app122412707

Baqeel, H., & Saeed, S. (2019, April). Face detection authentication on smartphones: End users usability assessment experiences. In 2019 International Conference on Computer and Information Sciences (ICCIS) (pp. 1-6). IEEE. https://doi.org/10.1109/ICCISci.2019.8716452

Im, J. H., Jeon, S. Y., & Lee, M. K. (2020). Practical privacy-preserving face authentication for smartphones secure against malicious clients. *IEEE Transactions on Information Forensics and Security*, *15*, 2386-2401. https://doi.org/10.1109/TIFS.2020.2969513

Iyanda, A. R., & Fasasi, M. E. (2022). Development of two-factor authentication login system using dynamic password with SMS verification. *International Journal of Education and Management Engineering*, *12*(3), 13. https://doi.org/10.5815/ijeme.2022.03.02

Oudah, M. S., & Maolood, A. T. (2022). Lightweight authentication model for iot environments based on enhanced elliptic curve digital signature and Shamir secret share. *International Journal of Intelligent Engineering & Systems*, *15*(5). chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://inass.org/wp-content/uploads/2022/03/2022103108-2.pdf

Pandey, S., & Bhushan, B. (2024). Recent Lightweight cryptography (LWC) based security advances for

https://doi.org/10.24191/jcrinn.v10i1.496

resource-constrained IoT networks. *Wireless Networks*, *30*(4), 2987-3026. https://doi.org/10.1007/s11276-024-03714-4

Pangan, A. M. S., Lacuesta, I. L., Mabborang, R. C., & Ferrer, F. P. (2022). Authenticating data transfer using RSA-generated QR codes. *European Journal of Information Technologies and Computer Science*, *2*(4), 18-30. https://doi.org/10.24018/compute.2022.2.4.73

Yaswanth, A., & Reddy, K. T. (2023). A novel dynamic randomized secret key model based on one-time password authentication. *International Journal of Intelligent Systems and Applications in Engineering*, *11*(3), 850-858.

Zakaria, A. A., Ab Halim, A. H., Ridzuan, F., Zakaria, N. H., & Daud, M. (2022). LAO-3D: A symmetric lightweight block cipher based on 3d permutation for mobile encryption application. *Symmetry*, *14*(10), 2042. https://doi.org/10.3390/sym14102042

About the Authors

Azni Haslizan, PhD is an Associate Professor in the Information Security and Assurance Programme at the Faculty of Science and Technology, Universiti Sains Islam Malaysia (USIM). She earned her PhD in Computer Science from Universiti Teknikal Malaysia Melaka (UTeM), a Master's in Digital Communication from Monash University, Australia, and a Bachelor's in Computer Information Systems from Bradley University, USA. Currently serving as Deputy Dean (Research and Innovation) at USIM, she is widely recognized for her expertise in cryptography, data privacy, and wireless security. With numerous publications and 10 innovation medals to her credit, she actively contributes to academia and serves on editorial boards, including OIC-CERT Journal and the Journal of Machine Intelligence and Computing. She can be reached through her email at ahazni@usim.edu.my.

Sakiinah Altaf Hussain is a Master of Science student at Universiti Sains Islam Malaysia (USIM), with a Bachelor of Science in Information Security and Assurance from the same institution. Her research interests lie in cybersecurity, where she focuses on exploring innovative solutions to address emerging digital threats. Sakiinah is passionate about advancing knowledge in information security and actively engages in research within the field. She can be reached through her email at sakiinah.fst@gmail.com.

Najwa Hayaati Mohd Alwi, PhD is an Associate Professor in Information Security at Universiti Sains Islam Malaysia (USIM). She earned her PhD from Cranfield University in 2012 and is a certified 1Citizen trainer, ISMS Internal Auditor, and Digital Leadership Educator. A member of the Malaysian Higher Education Teaching and Learning Council, she was also a part of the Malaysia E-learning Council (2013-2018). Appointed as Deputy Director for USIM's Centre of Excellence for Teaching and Learning in 2021, her expertise spans information security, digital content, and socio-technical research. S is also a certified Cyber Defender Associate and Data Protection Officer. She can be reached through her email at najwa@usim.edu.my.