CHAPTER 5

USER-DEVICE AUTHENTICATION MODEL EVALUATION

5.1 Overview

This chapter discusses the evaluation of the User-Device Authentication Model with Digital Certificate for Smartphone User. The research is done using Qualitative Research, thus, there are two ways to evaluate the User-Device Authentication Model which are by collecting respondents from experts' reviews and calculating the mathematical formula used in the model to produce the expected outcome. The core objective of the evaluation is to observe whether this model is workable after getting reviews from experts, and suggestions for improvement of the model and to ensure that the results are in line with the expected outcome. This will ensure that the User-Device Authentication Model can be applied for implementation and be used by society.

5.2 Proposed Authentication Model Validation

The research aimed to investigate the User-Device Authentication Model utilizing Digital Certificates for Smartphone Users and gather expert feedback on its effectiveness. Experts with extensive knowledge of smartphone authentication principles were consulted and their opinions were categorized into three main areas: registration, certificate issuance, and authentication/validation phases.

The model was designed to prioritize smartphone security, allowing users to protect their data and prevent unauthorized access and fraudulent activities. It is expected to improve user experience by removing the need for additional authentication measures. By authenticating both the user and device, the model has the potential to enhance user experience by potentially eliminating the need for repeated authentication after the initial authorization process.

5.3 Expert Review Evaluation

For the Expert Review Evaluation, meeting face-to-face and online meetings with the experts were done to present the User-Device Authentication Model and get their feedback and suggestions regarding the User-Device Authentication Model. This evaluation is done to determine whether the User-Device Authentication Model can be used for application purposes. Expert Review Evaluation requires the experts to answer questionnaires after they have been explained the concept of the User-Device Authentication Model. This User-Device Authentication Model has been evaluated by 8 respondents who are among academia and industry who are authentication experts. The list of questions used in this user evaluation is in Appendix C: Questionnaires User-Device Authentication Model with Digital Certificate for Smartphone User. There are two versions of the forms which are in PDF Form and Google Form. The Experts can choose either form for answering the questionnaires. There are three phases of this Model and each question is associated with those phases.

The experts have a wide range of experience in the security of information systems, including working in the security domain in computer centers, publishing

many security articles and teaching various security courses as well as vast knowledge in authentication implementation at the industry level. On the other hand, the experts are professors at the university which allows them to know the security issues of the current information system at the university as well as experts from the industry that can give their insight regarding the architecture of the proposed model. Table 5.1 lists all the expert reviews that evaluate the User-Device Authentication Model.

Table 5. 1: Experts Review Details

Name	Job Position/Expertise	Company Name	Years of Experience
Dr. Abdul Alif Zakaria	Senior Analyst/ Information Security	Cybersecurity Malaysia	13
Dr. Iznora Aini Zolkifly	Senior Lecturer/ Cybersecurity, Computer Graphics	UNITAR International University	24
Mr. Mas Hairul Rasyidi	Software Developer	Net Byte Security	3
Dr. Nur Hafiza Zakaria	Lecturer	Universiti Sains Islam Malaysia (USIM)	5
Dr. Noorul Halimin Mansol	Freelance Auditor	SIRIM QAS Sdn. Bhd	23
Dr. Azuan Ahmad	Lecturer	Universiti Sains Islam Malaysia (USIM)	5
Mr. Akhmal Marsidi	IT Security Architect	Orstead Malaysia	27
Nur Syafiqah Mohd Shamsuddin	Digital Forensics Quality Assurance and Analyst	Malaysian Communications and Multimedia Commission (MCMC)	4

5.4 Data Collection

The following techniques were used to guarantee that the data collection and evaluation were effective. First, the researcher explained the purpose of the questionnaire, went into detail about its process, and emphasized how important it was that respondents give thoughtful answers. Additionally, the responses obtained from the respondents were grouped using a five-point Likert scale, which includes grades ranging from one representing strong disagreement to five representing strong agreement. This scale produced more discernible reactions than scales with fewer gradations because of its increased density compared to lesser scales. Lastly, Table 5.2 provides evidence that the questionnaire data-collecting procedure met the qualitative standard outlined in the research by Mellenbergh et al. (2003), which is an important factor in the construction of instruments.

Table 5. 2: Criterion Degree for Each Level of Answers

Scale Index	Answer	Answer Level
1-1.45	Strongly Disagree	Very low
1.5-2.49	Disagree	Low
2.5-3.49	Neutral	Medium
3.5-4.49	Agree	High
4.5-5	Strongly Agree	Very High

The data was extracted both physically and digitally using PDF Answer Sheets and Google Form Sheets and carefully transferred into Excel 2021 software.

There are many phases involved in the analysis of completed surveys. First, a series of pre-written questions is created that are divided into three phases and include several sub-questions to thoroughly cover the fundamental elements of the subject under study. The researcher then carefully reviews the replies that were submitted, reviewing

them multiple times to make sure that they are correct and comprehensive. Subsequently, the gathered questionnaire responses undergo a systematic assessment, and the results relevant to every topic are calculated and combined. Both the in-presentation and questionnaire-based replies are subject to this synthesis process. The total results are collated and presented after each component of the questionnaire replies has been carefully examined.

5.5 Questionnaire Reliability

The reliability of questionnaire data is defined by Bränström *et al*. (2002) as the relationship between responses. Responses that have been carefully filled out are more reliable than those that were filled out randomly. Cronbach's alpha is one of the most reliable tests for quantitative data reliability. If the reliability of the data is higher than 0.7 according to Cronbach's alpha, it's considered acceptable. Table 5.3 below shows the calculation done to calculate Cronbach's alpha using Microsoft Excel. The formula used to calculate the Cronbach's alpha as follows:

$$\alpha = \left(\frac{k}{k-1}\right)\left(\frac{s_y^2 - \sum s_i^2}{s_y^2}\right)$$

(Equation 5. 1): Cronbach's alpha.

Where:

α = Cronbach's alpha

k = number of questionnaires

s_y^2 = Variance of the total scores of each question.

s_i^2 = Variance of each question.

To calculate the value of the variance of each question, the following formula is used.

$$the\ e\ s_i^2 = \frac{\sum(x_i - \overline{x})^2}{n-1}$$

(Equation 5. 2): Variance of each question

Where:

s_i^2 = Variance of each question.

i= Number of individual questions

$\sum x_i$ = sum of data questions

x = mean of data questions

n = number of individuals

Based on the equation above, the value squared for Question one is as follow:

$$:s_i^2 = \frac{\begin{matrix}(5-\overline{4.875})^2+(5-\overline{4.875})^2+(5-\overline{4.875})^2+\\(4-\overline{4.875})^2+(5-\overline{4.875})^2+\\(5-\overline{4.875})^2+(5-\overline{4.875})^2+(5-\overline{4.875})^2\end{matrix}}{8-1}$$

(Equation 5. 3): Variance of Question One

Based on the calculation above, the variance for question number one is 0.125. The formula above is used to calculate the variance for question number two until question number 15 and the value of variance can be found in table 5.3 below.

The same method is used to calculate the variance of total scores of each question, s_y^2 and the value of variance can be found in table 5.3 below.

Based on the formula Cronbach's Alpha 1.8 above, to calculate Cronbach's alpha is as follows:

$$\alpha = \left(\frac{15}{15-1}\right)\left(\frac{50.78571-6.25}{50.78571}\right) = 0.939572031$$

(Equation 5. 4): Cronbach's alpha for the Proposed model questionnaires

Therefore, the questionnaire results are accurate and can provide insight into the true state of opinion of respondents. This shows that the questionnaires are reliable and can be used to measure the functions of the proposed Authentication Model based on the answers provided by the experts from academicians and industrial experts.

Table 5. 3: Calculation of Cronbach's alpha.

Questionnaires (Q)																
Individual	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Total
1	5	5	4	5	5	4	5	4	5	5	5	4	5	5	5	71
2	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	61
3	5	5	5	5	5	5	5	4	4	5	5	5	5	5	4	72
4	4	4	3	4	4	4	4	3	4	4	3	4	3	4	4	56
5	5	5	3	4	4	4	3	4	4	4	4	3	4	3	3	57
6	5	5	5	5	5	5	5	4	5	5	5	5	5	5	5	74
7	5	5	4	4	4	4	5	4	5	5	5	5	5	5	5	70
8	5	5	5	4	4	5	4	5	4	5	3	5	5	5	5	69
														Total Variance		50.78571

Variance	0.125	0.214286	0.696429	0.267857	0.267857	0.553571	0.285714	0.267857	0.267857	0.785714	0.553571	0.571429	0.571429	0.553571	6.25
Cronbach's Alpha Value													0.939572031		

5.6 Questionnaire Results from Expert Reviews

This subtopic explains the result of each questionnaire from eight experts as well as the explanation of each of the questions. There are three phases for the proposed model that are being answered by the experts.

5.6.1 Registration Phase Evaluation

Below is the list of questions provided in the questionnaires for the experts to answer and analysis of the answers from the experts for each 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.

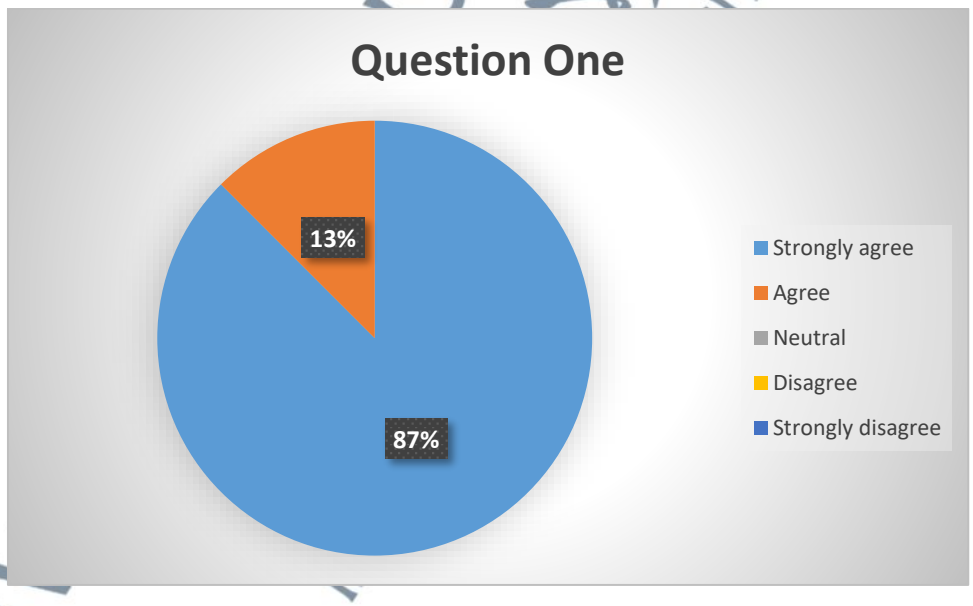


Figure 5. 1: Pie Chart of Results in Question 1.

For question 1, based on the pie chart shown in Figure 5.1, the results show that 87% of experts agree that it is more secure to authenticate both user and device rather

than the user. This is because authenticating both the user and the devices can enhance the security where this approach provides an additional layer of protection by verifying the identity of the user and the device, they are accessing the system from. It guarantees that the user is using a reliable and secure device (Hussain & Jain, 2020). The ability to authenticate users and devices can protect against a variety of threats, including unauthorized access from unsecured devices, unauthorized access from compromised devices, and device spoofing (Zhu et al., 2020).

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.

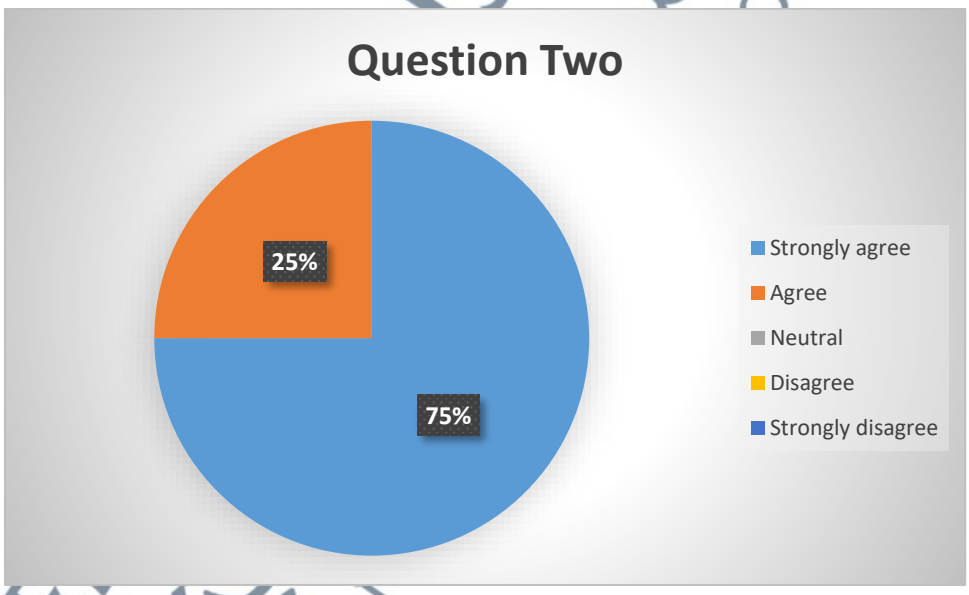


Figure 5. 2: Pie Chart of Results in Question 2

For question two, based on the pie chart shown in Figure 5.2, the results show that 75% of the experts agree that using two pieces of information to register the device is much more secure than registering one piece of information since the IMEI number is

the unique number only available to a device. Each device will contain two IMEI numbers since the majority of smartphones consist of two SIM card slots. These IMEI numbers are unique to only a device. It can avoid cloning of the smartphone where the attackers try to duplicate the legitimate user's device (Yu et al., 2018) (Hammood et al., 2020).

3. Using the Rivest–Shamir–Adleman (RSA) algorithm is suitable for generating public key and private key in smartphone user.

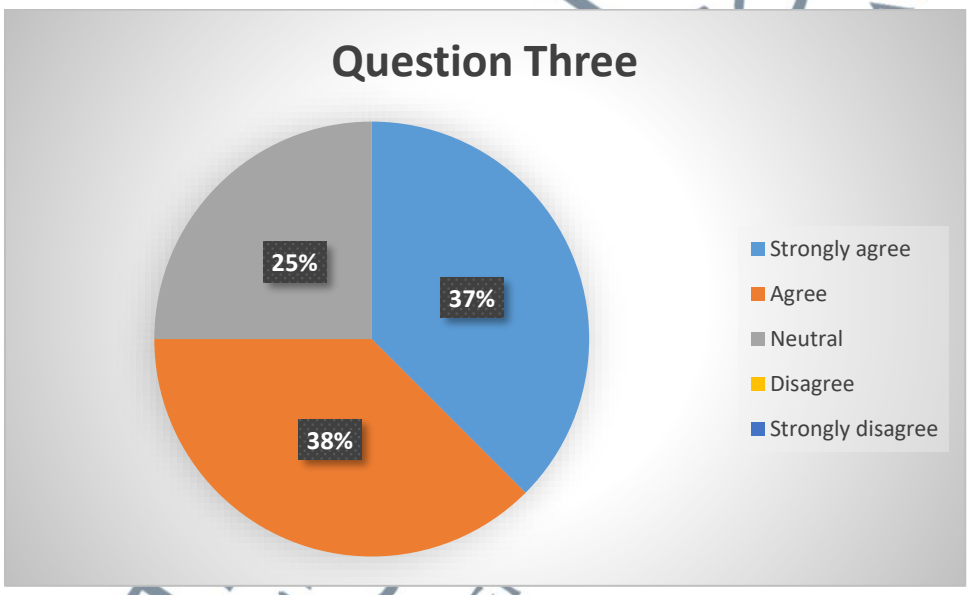


Figure 5. 3: Pie Chart of Results in Question 3

For question three, based on the pie chart shown in Figure 5.3 shows that 37% of the experts strongly agree that the RSA algorithm is suitable for generating public and private key whereas 38% agree with the fact mentioned. However, 25% of the experts are neutral about using the RSA algorithm for generating public and private key. The reason some of the experts choose neutral is due to having other better options besides RSA such as ECC. The researcher has chosen RSA as the algorithm used due

to the fact that it is widely used in crypto libraries and standards, making it one of the most popular interoperability partners. Many legacy systems and applications rely on RSA, making it easier to incorporate into legacy systems (Harsha & Patil, 2017). Besides, RSA has shorter signature generation and verification time compared to ECC (Alam, 2016) (Harsha & Patil, 2017) (Sinha et al., 2013).

4. Both the user and device need to be assigned their own pair of keys by the server after registering.

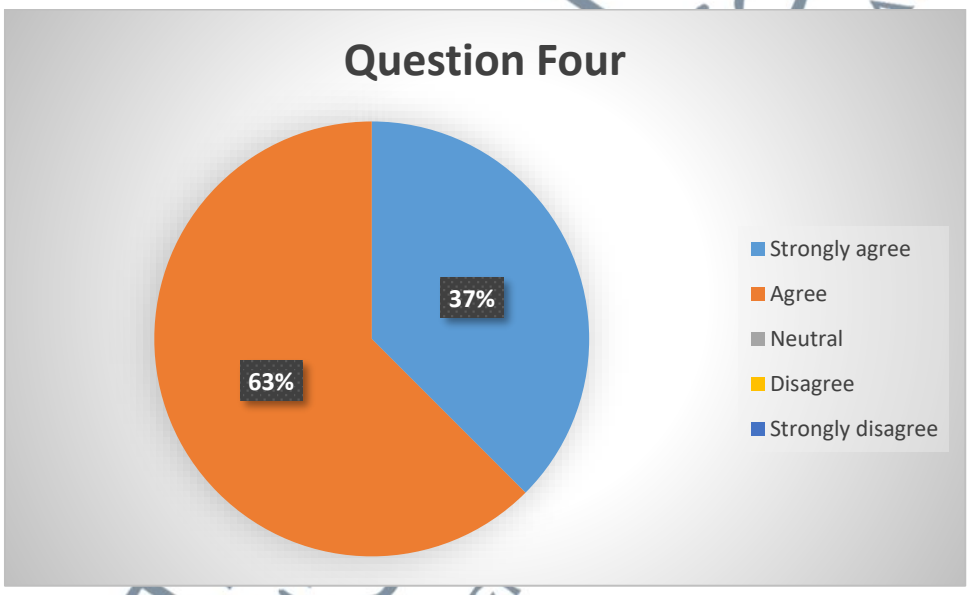


Figure 5. 4: Pie Chart of Results in Question 4

For question four, based on the pie chart shown in Figure 5.4 shows that 37% of experts strongly agree that both the user and the device need to be assigned their pair of keys while 63% of experts agree with the fact mentioned. The key assigned to each user and device is important to encrypt the user's and the device's information before sending it to the Certificate Authority (CA) to sign the encrypted information (Dharminder, 2019).

5.6.2 Digital Certificate Issue Phase Evaluation

5. Producing two digital certificates for the user and device respectively can enhance the authenticity of the user and device in smartphone applications.

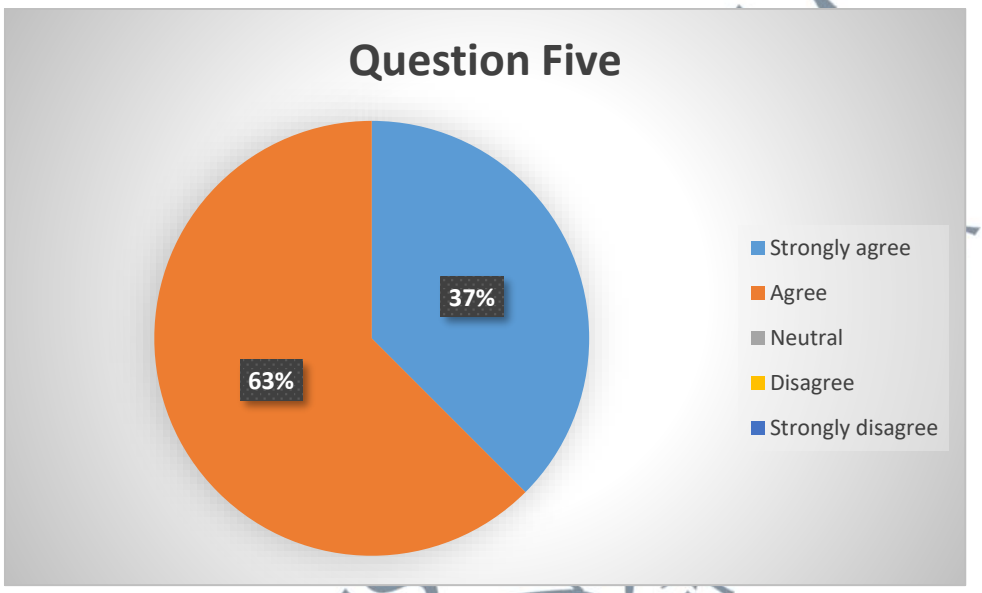


Figure 5. 5: Pie Chart of Results in Question 5

For question five, based on the pie chart shown in Figure 5.5 shows that 37% of experts strongly agree that producing two digital certificates for the user and the device can enhance the authenticity of the user and the device while 63% of experts agree with the fact mentioned. The utilization of distinct digital certificates for user and device authentication can offer increased security and scalability in a variety of contexts. By utilizing separate certificates, individual authentication can be achieved for both users and devices, allowing for more granular control over access to the system and independent verification of each entity. Additionally, Device certificates are capable of uniquely identifying and authenticating hardware devices, including Internet of Things (IoT) devices, server-based systems, and network equipment, thus ensuring that

authorized devices are only permitted to access a network or system (Karthikeyan et al., 2018) (Siddiqui et al., 2022).

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)

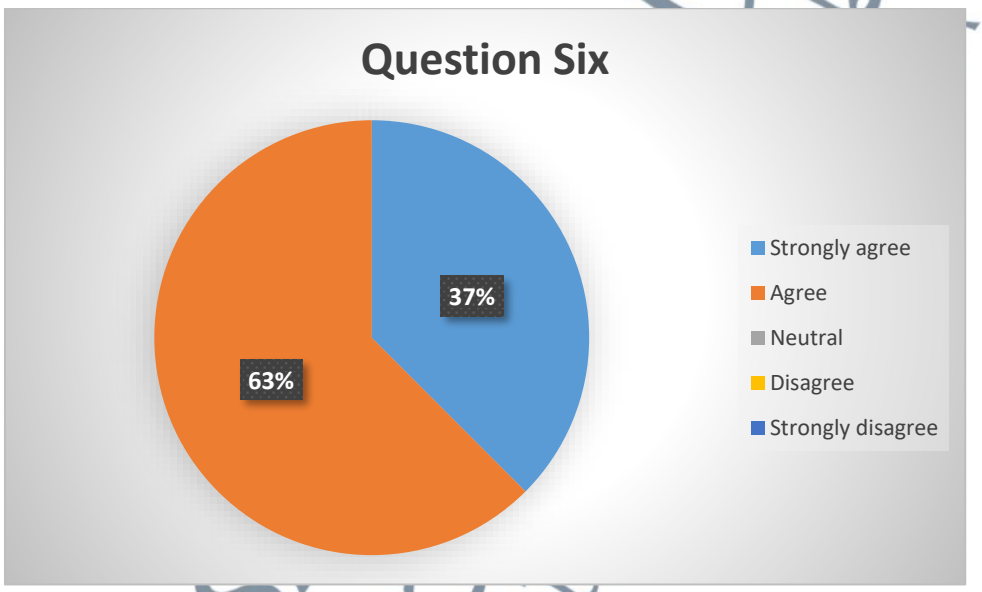


Figure 5. 6: Pie Chart of Results in Question 6

For question six, based on the pie chart shown in Figure 5.6 shows that 37% of experts strongly agree that a feasible solution to link both the user and their device is to incorporate information from both into a respective certificate whereas 63% agree on the fact above. Generally, the experts agree on having to link both the user and device's information for generating certificates. Signing encrypted information from the user followed by the device can secure the legitimacy of both the user and the device and avoid Man-in-the-Middle Attack. Even if a malicious actor intercepts the encrypted

message and attempts to change the content, the recipient can identify the change by checking the digital signature (Yuvaraj et al., 2022).

7. Using two digital certificates from both the user and the authentication device is better for securing smartphone applications.

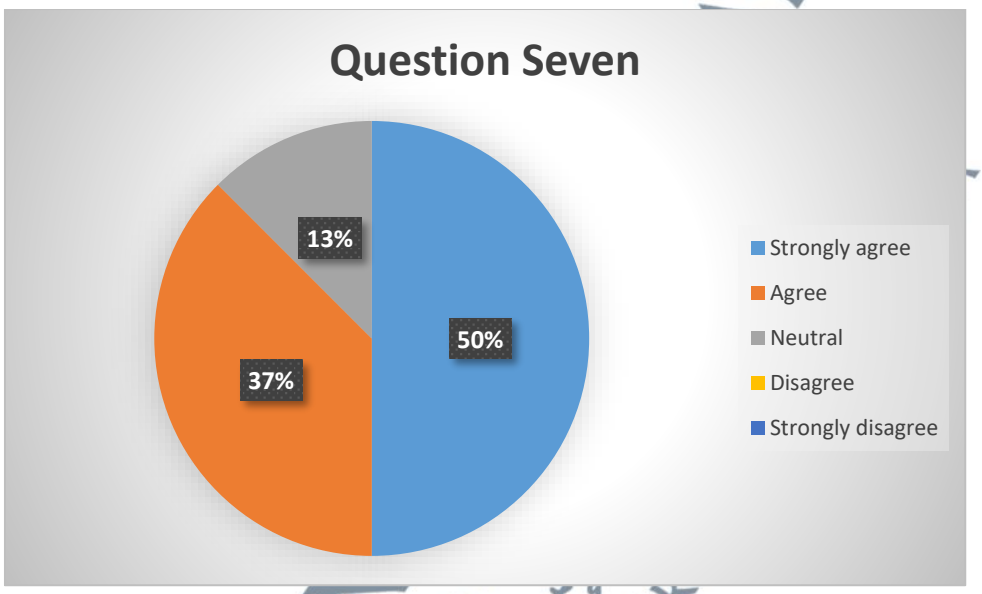


Figure 5. 7: Pie Chart of Results in Question 7

For question seven, based on the pie chart shown in Figure 5.7 shows 50% of the experts strongly agree while 37% of experts agree that having two digital certificates to authenticate both the user and the device is better for securing smartphone applications. Whereas 13% of the experts are neutral with the fact mentioned. The reason of the expert to choose neutral is due to the complexity of generating the digital certificate and since there are two digital certificates, the complexity of authentication using digital certificates is higher. The implementation of two-factor authentication (2FA) in smartphone applications can be enhanced by the combination of user and device certificates. This is especially beneficial in situations where robust

authentication and access control are essential. By combining user and device certificates, users can access the application with both a user certificate (user's certificate) and a device certificate (device certificate), which is more secure than relying on a single password or PIN (Chifor et al., 2018) (Almajali et al., 2018).

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.

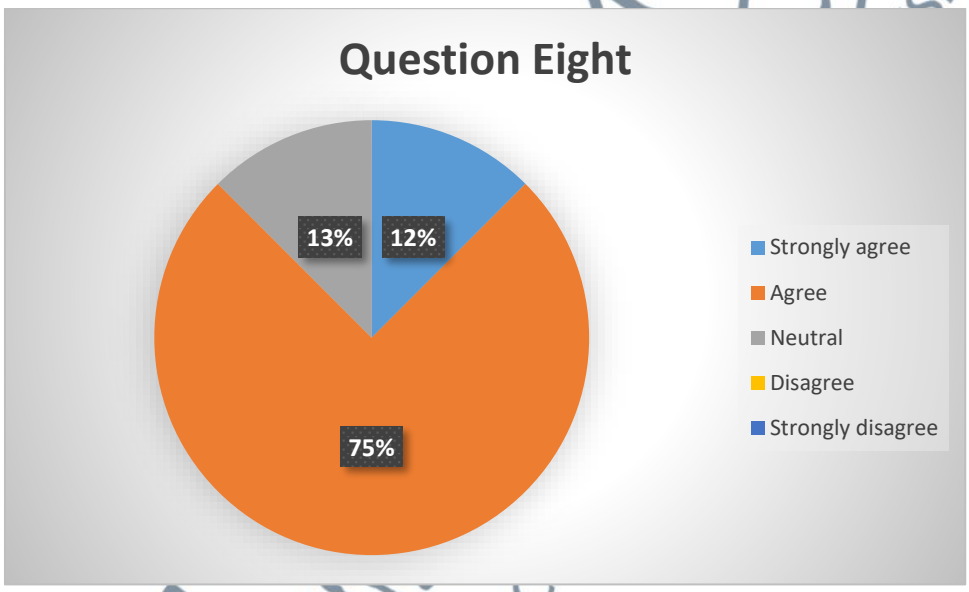


Figure 5. 8: Pie Chart of Results in Question 8

For question eight, based on the pie chart shown in Figure 5.8 shows 12% of the experts strongly agree and 75% agrees that the certificate issued by the CA must have a time limit to stay as valid. 13% of the experts are neutral since they believe Digital certificates need to be updated regularly since they expire. If renewal procedures are not managed effectively, this process may be difficult and lead to security problems. Verification problems may arise if the CA's public key certificate expires and is not renewed.

. The setting of an expiration date on digital certificates offers several advantages for security and management. Expiring certificates promote regular key updates, as certificates can be renewed or replaced, resulting in the generation of new cryptographic keys. This safeguards against potential attacks that focus on long-term key weaknesses or exploits that have been identified after the issuance of the certificate. Additionally, the expiration date requires certificate holders to go through a verification process regularly, ensuring that the identity of the holder of the certificate is still valid and can be verified (Siddiqui et al., 2022).

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.

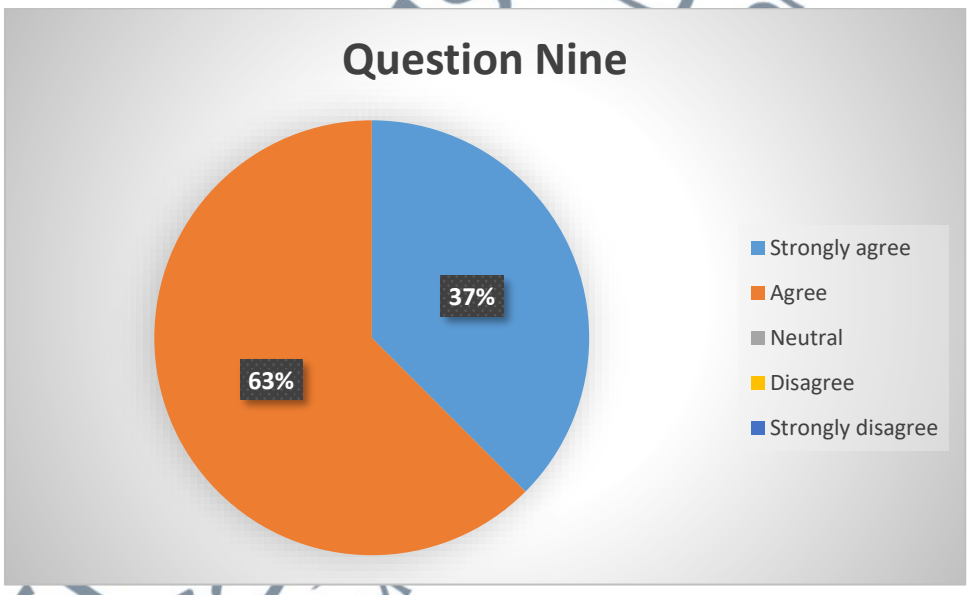


Figure 5. 9: Pie Chart of Results in Question 9

For question nine, based on the pie chart shown in figure 5.9 shows 37% of the experts strongly agree and 63% agree that using the Certificate Authority (CA) for signing the User and Device's certificate is better for protecting the key of the user and device from unauthorized access. To improve security and safeguard user and device

keys from unauthorized access, a common and effective solution is to enlist the services of Certificate Authorities (CAs). CAs typically use secure key generation practices when creating certificates for users and devices. This involves securely generating the associated private key and storing it in a secure environment, thus ensuring that the key is not compromised during the generation process. Additionally, the centralization of certificates and keys is facilitated by the use of a CA, which facilitates the issuance, renewal, and revocation of certificates, thus simplifying the process of maintaining security policies and responding to security incidents (Poorni et al., 2019) (Roy & Karforma, 2014).

5.6.3 Authenticate/Verification Phase Evaluation

10. Double authentication using user and device signature is more secure compared to single authentication in smartphone applications.

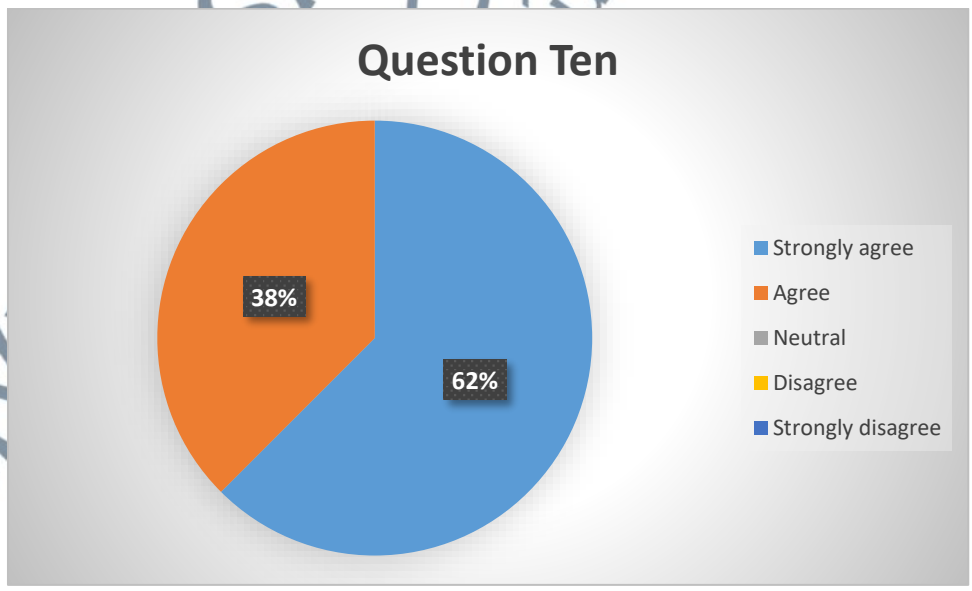


Figure 5. 10: Pie Chart of Results in Question 10

For question ten, based on the pie chart shown in figure 5.10 shows 62% of the experts strongly agree and 38% agrees that double authentication using user and device signature is more secure compared to single authentication in smartphone applications. The implementation of double authentication in smartphone applications, which involves the use of both a user signature and a device signature, can significantly increase the security of an account. This method combines the advantages of 2FA and adds a layer of protection. Double authentication confirms the identity of both the user and the device, thus reducing the likelihood of account compromise caused by stolen credentials. Furthermore, even if an attacker were to acquire the user's credentials, the authorized device would still need to be authorized for the authentication process to be completed. This further reduces the risk of unauthorized devices being used to gain access to the application (Liu et al., 2020) (Ramesh et al., 2022).

11. Using Certificate Authority's Public key, Kpub(ca) to verify the signature can avoid unauthorized access in smartphone applications.

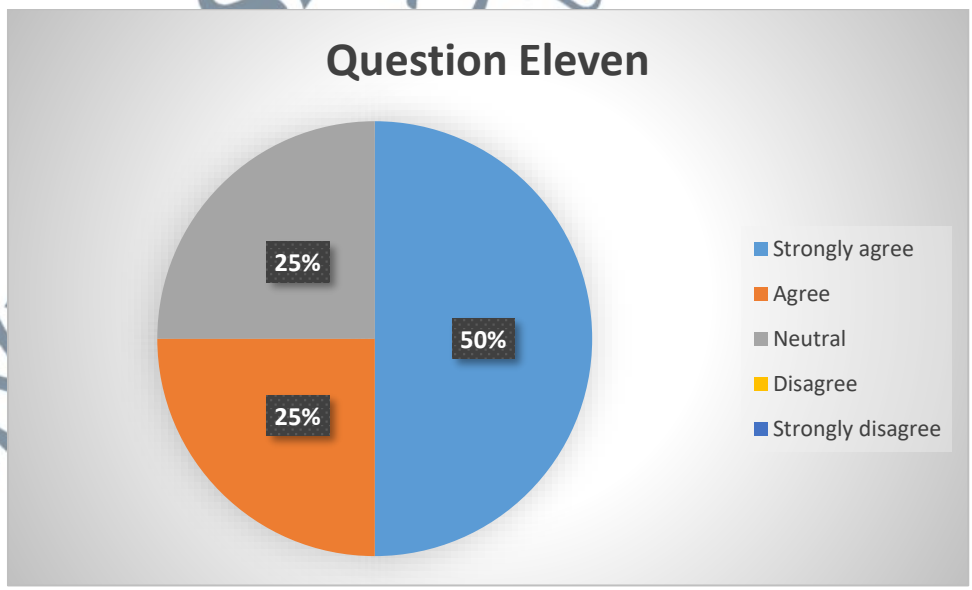


Figure 5. 11: Pie Chart of Results in Question 11

For question eleven, based on the pie chart shown in figure 5.11 shows that 50% of the experts strongly agree and 25% agree that using Certificate Authority's Public key, Kpub(ca) to verify the signature can avoid unauthorized access in the smartphone application. 25% of the experts are neutral on this fact. This might be due to the CA is critical to the overall system's security. Attackers can construct phony digital signatures, impersonate entities, and issue fraudulent certificates if the CA is hacked or if its private key is exposed. This leads to a breakdown of trust in the whole Public Key Infrastructure (PKI).

The use of a Certificate Authority's Kpub(ca) public key to authenticate digital signatures in smartphone applications can improve security and reduce the risk of unauthorized access. Before receiving an incoming message or request, the smartphone application and the user will verify the digital signature using Kpub(ca). This ensures that the message has been signed with the private key attached to the CA-issued certificate. Furthermore, if the signature is verified, the smartphone app and the user can be assured that the message is sent by a legitimate person with a valid CA certificate. This enables the application to verify the user or device, granting access based on the user's permissions and roles (Ramesh et al., 2022) (Roy & Karforma, 2014).

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.

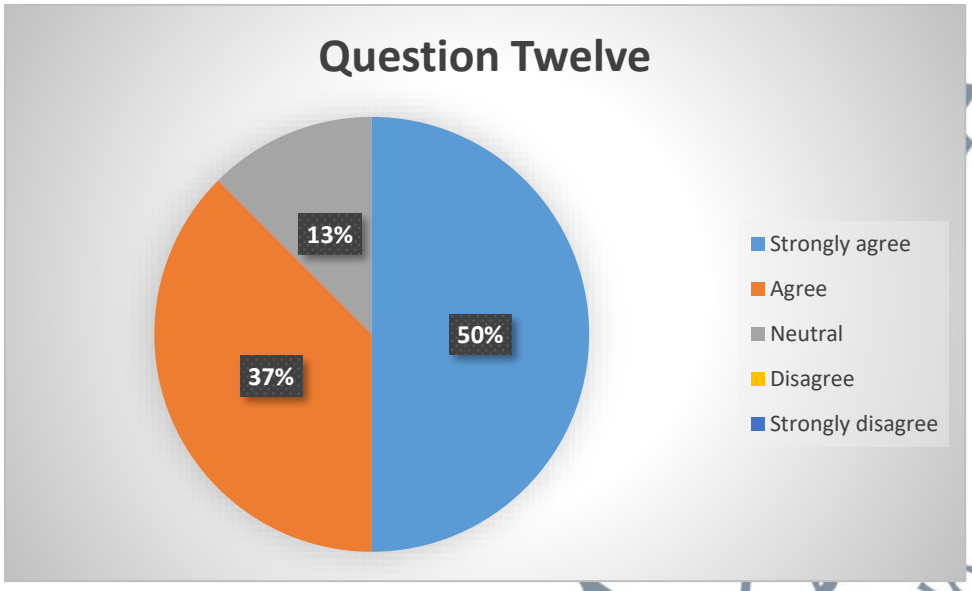


Figure 5. 12: Pie Chart of Results in Question 12

For question twelve, based on the pie chart shown in figure 5.12 shows that 50% of the experts strongly agree and 37% of the experts agree that 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. Calculating separately will ensure that the calculation will run smoothly as well as ensure that the decrypted information is legitimate.

5.6.4 General Question

13. All three phases in the model are sufficient to ensure strong authentication for smartphone applications.

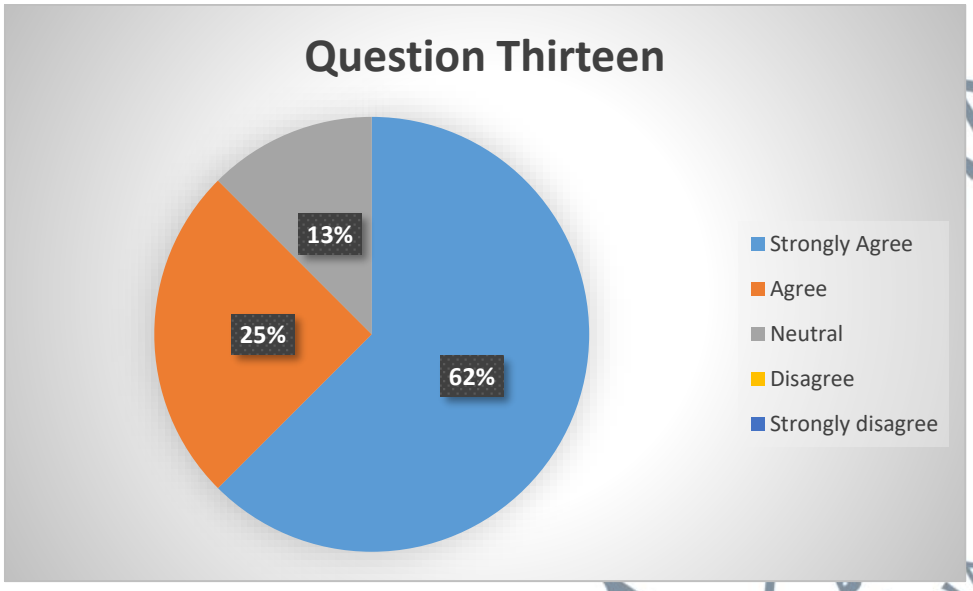


Figure 5. 13: Pie Chart of Results in Question 13

For question thirteen, based on the pie chart shown in figure 5.13 shows that 62% of the experts strongly agree and 25% of the experts agree that all three phases involved in the proposed model are sufficient to ensure strong authentication for smartphone applications.

14. All the authentication factors which are user, device, and Certificate Authority can ensure strong authentication for smartphone applications.

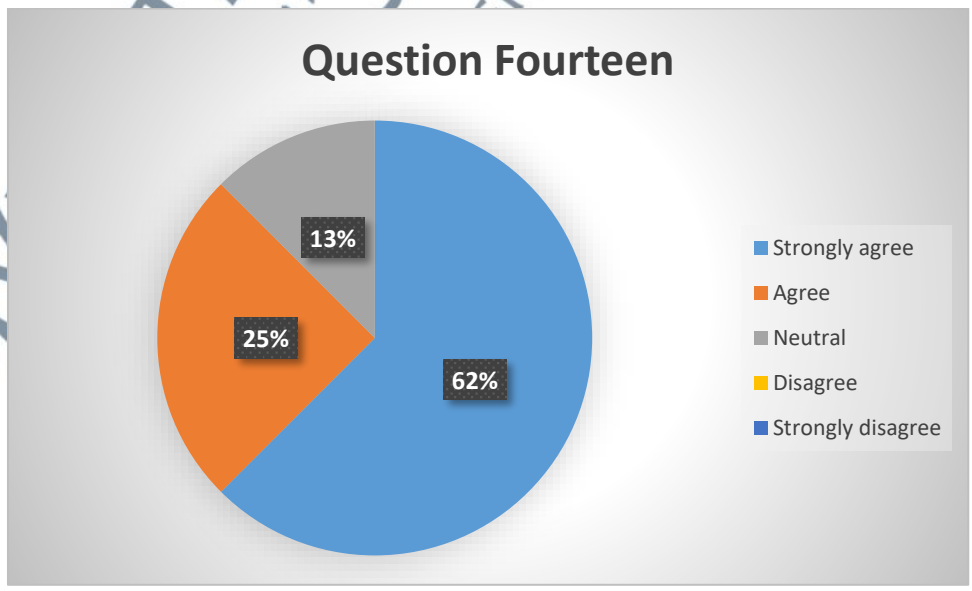


Figure 5. 14: Pie Chart of Results in Question 14

For question fourteen, based on the pie chart shown in figure 5.14 shows that 62% of the experts strongly agree and 25% of the experts agree that all the authentication factors which are user, device, and Certificate Authority can ensure strong authentication for smartphone application.

15. This model is suitable to be applied in smartphone applications.

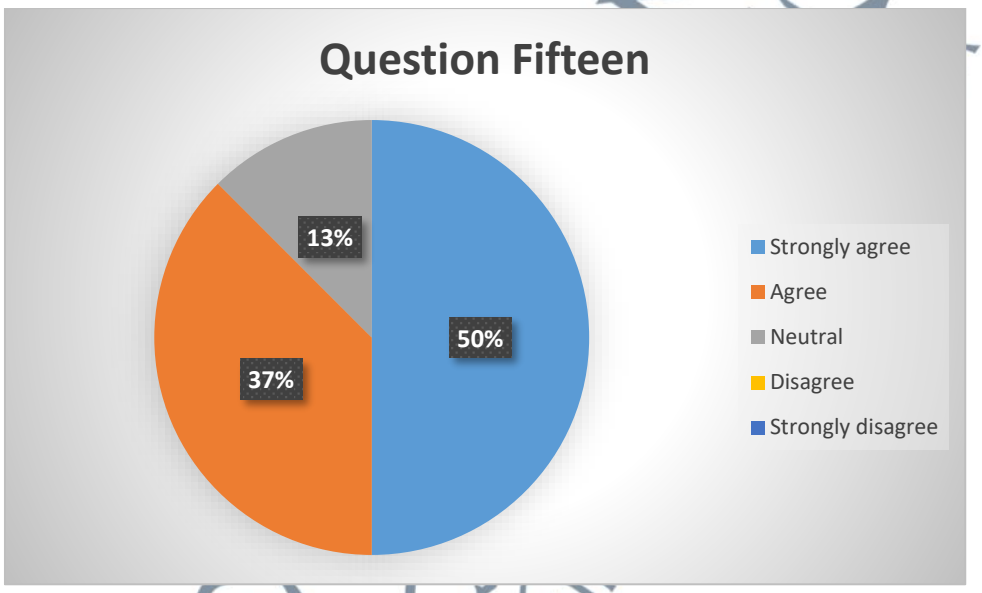


Figure 5. 15: Pie Chart of Results in Question 15

For question fifteen, based on the pie chart shown in figure 5.15 shows that 50% of the experts strongly agree and 37% of the experts agree that the proposed model is suitable to be applied in the smartphone application.

5.6.5 Comments and Suggestions from Experts

There are a few suggestions given by the experts to improve the functionality of the User-Device Authentication Model.

Table 5.4 shows the comments and suggestions given by all the experts based on each of the questions in the questionnaire.

Table 5. 4: Comments and Suggestions Given by the Experts Review.

Experts Name	Number of Questions	Comments/Suggestions
Dr. Abdul Arif Zakaria	8	He suggests that for the Certificate Authority (CA) to renew the certificate for the user, the user must be assigned new pairs of keys before renewing the certificate.
Mr. Mas Hairul Rasyidi	5	He questioned what if the device used is a virtual device such as an Emulator and virtual machine.
Dr. Iznora Aini Zolkifli	3	She commented that the RSA algorithm can generate keys of varying lengths, and longer keys provide higher security. However, longer keys also require more computational power, which can be a concern for mobile devices with limited processing power and battery life. She suggests choosing the key length carefully based on the security requirements and the capabilities of the target device.
	5	She commented that by issuing separate digital certificates for the user and device, it is possible to verify the authenticity of both parties independently. However, producing and managing multiple digital certificates can also increase complexity and cost.
	8	She suggested implementing an automated certificate renewal process, so the system can ensure that certificates are always up to date and that users can continue to access the system without interruption. This process can improve security by ensuring that only valid certificates are used to access the CA must be fully aware to notify the user and administrator when a certificate is about to expire

	11	She commented that using the CA's public key can also help to prevent unauthorized access by ensuring that only legitimate users with valid certificates can access the system.
	12	She commented that the type of data being accessed, the potential risks of unauthorized access, and the capabilities of the devices and users involved should be considered when designing the authentication process.
	15	She commented that this model is suitable to be applied in smartphone applications, especially in situations where high security is required.
Dr. Noorul Halimin	2	She commented that to her knowledge, the IMEI number is also used by the manufacturer to avoid connection to the network for stolen phones. Also, she told to consider if the smartphone has two sims that have 2 different IMEI numbers.
	3	She suggests considering the use of Elliptic Curve Cryptography (ECC) for mobile use.
	6	She commented that to her knowledge, using email user (during the registration phase) is very low assurance of a digital certificate. She suggested considering proposing a high level of assurance by using an NRIC/passport number to create a user ID.
	8	She suggested consider propose the short-term validity certificate where the certificate will be purged once been used.
	12	She suggested considering the time taken for the verification process for example verification with a Certificate Revocation List (CRL).
Dr. Azuan Ahmad	1	He commented that registering the device and user ensures the authenticity of the user by requiring both the user and device available at the same time

	2	He commented that IMEI is a unique identifier for each mobile phone while phone numbers can be cloned or used on different devices.
	8	He commented that for application purposes, it will incur costs from the user.
	15	He suggested considering user friendliness or including an additional authentication mechanism in case the user lost their phone
Mr. Akhmal Marsidi	1	He commented that two-factor authentication (2FA) is more secure compared to single-factor authentication example password-only
	3	He commented that ECC seems to be more efficient than RSA but RSA is more popular.
	4	He commented that Private keys need to be with the user. CA should only process the user's CSR (certificate request). Disagree with CA to generate a key pair for users. He also commented that key pairs can be used for different functions i.e. one for data encryption and the other key pair for digital signature. A single key pair can be used for data encryption & digital signature as well.
	5	He commented that he agrees for two certificates to be produced provided that one certificate is for the user and the other is for the device.
	6	He commented that both certificates have the same info. Using any of the certs will lead to the same object (user with device)
	7	He suggested that the application should be able to verify or link both users and devices authenticated using their digital certificate. i.e., 'cert-user AND cert-device' instead of 'cert-user OR cert-device' to allow access

	8	He questioned whether the key pair generated automatically as well. And he also asks who regenerates the key pair. He mentioned that CA typically processes certificate requests from a user or device and then generates a digital signature.
	9	He commented that the key must be stored by the user.
	12	He suggested using Boolean where to allow only with Cert-user AND cert-device
	13	He commented that the Private key should be with the user and never with the CA
	14	He commented strong authentication can be implemented with correct implementation and private key with the user
	15	He commented this model can be applied to smartphone applications provided the correct implementation and private key with a user
Ms. Nur Syafiqah Mohd Shamsuddin	3	She commented that the performance shall be considered while using RSA Algorithm.
	7	She commented that the performance of the applications in smartphones might differ from one another
	12	She commented that either way whether authenticating the user first or the device first yields the same results.
	15	She commented that this model is not necessarily to be implemented into smartphone applications only, there is also a wide range of other computer applications that should be implemented using this method.

Based on the comments above, some justification can be explained regarding the proposed model. Some experts suggest using ECC instead of RSA for digital signature generation. The proposed model using RSA algorithm because RSA signature generation is essentially the process of raising a big integer to the power of the exponent

of the private key. Because the RSA private keys may be selected with tiny exponents, which speeds up the signature creation process, this procedure is efficient. Compared to the straightforward exponentiation used in RSA, the elliptic curve point multiplications involved in ECC signature production are more mathematically difficult. To create a signature using ECC, a point on an elliptic curve must be multiplied by a big scalar, particularly the private key. This needs additional processing processes.

5.7 Mathematical Calculation Based on the Algorithm Used in the Proposed Model

To determine whether the suggested model is effective in producing the expected outcomes, simulated data is utilized to calculate the expected result by utilizing the algorithm that is inherent to the suggested model. The first stages entail calculating the public and private keys for the user, device, and Certificate Authority (CA).

5.7.1 Simulated Data One

First step, to calculate the value of two prime numbers, n, the following equation is used.

$$n = p \,.\, q$$

(Equation 5. 5): Value of two prime numbers, n.

Next, the Euler's Totient, Φ(n) is calculated to obtain the public exponential, e. The formula below is used to calculate the Euler's Totient, Φ(n).

$$\Phi(n) = (p-1)(q-1)$$

(Equation 5. 6): Euler's Totient, Φ(n).

The public exponential, e, is selected by e ∈ {1,2, . . . , Φ(n)−1} such that gcd(e,Φ(n)) = 1

Once the public exponential is determined, the private key, d is calculated using the following formula.

$$d \cdot e \equiv 1 \, mod \Phi(n)$$

(Equation 5. 7): Private Key, d.

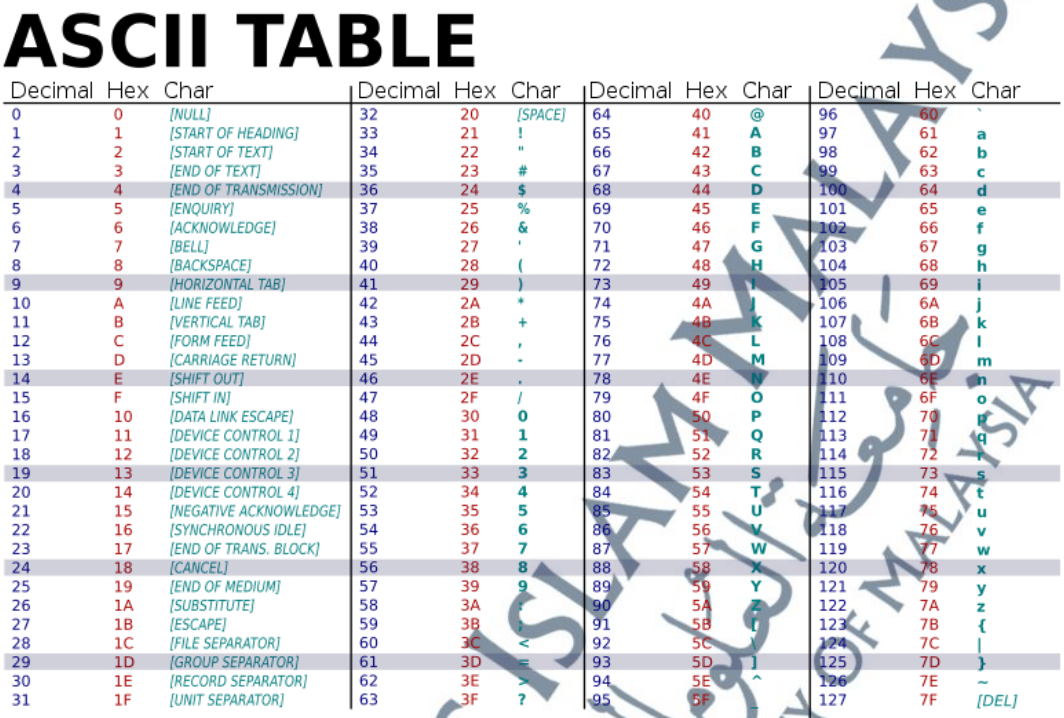
Thus, the value of the Public Key of user, Kpub(u) = (n, e), and the private key of the user, Kpr(u) = d. Table 5.5 below shows the value of p, q, n, Φ(n), e, and d for user, device, and certificate authority (CA) respectively.

Table 5. 5: Value of p and q for User, Device, and CA for First Simulated Data.

Prime value	User (U)	Device (D)	Certificate Authority (CA)
p	3	7	11
q	11	19	13
n	33	133	143
Φ(n),	20	108	120
Public key (n,e)	(33,7)	(133,7)	(143,7)
Private key (n,d)	(33,3)	(133,13)	(143,43)

The first simulated date chosen for UserID is '*test*' and the device IMEI number is 3584. These two pieces of information need to be converted to decimal value using the ASCII Table shown in Figure 5.16. The word 'test' is converted to 116 101 115 116 and the IMEI number 3584 is converted to 51 53 56 52. These values must be encrypted

using the public key of the user and device respectively. The calculation is done using Omni Calculator.



ASCII TABLE

Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char	Decimal	Hex	Char
0	0	[NULL]	32	20	[SPACE]	64	40	@	96	60	`
1	1	[START OF HEADING]	33	21	!	65	41	A	97	61	a
2	2	[START OF TEXT]	34	22	"	66	42	B	98	62	b
3	3	[END OF TEXT]	35	23	#	67	43	C	99	63	c
4	4	[END OF TRANSMISSION]	36	24	$	68	44	D	100	64	d
5	5	[ENQUIRY]	37	25	%	69	45	E	101	65	e
6	6	[ACKNOWLEDGE]	38	26	&	70	46	F	102	66	f
7	7	[BELL]	39	27	'	71	47	G	103	67	g
8	8	[BACKSPACE]	40	28	(	72	48	H	104	68	h
9	9	[HORIZONTAL TAB]	41	29	)	73	49	I	105	69	i
10	A	[LINE FEED]	42	2A	*	74	4A	J	106	6A	j
11	B	[VERTICAL TAB]	43	2B	+	75	4B	K	107	6B	k
12	C	[FORM FEED]	44	2C	,	76	4C	L	108	6C	l
13	D	[CARRIAGE RETURN]	45	2D	-	77	4D	M	109	6D	m
14	E	[SHIFT OUT]	46	2E	.	78	4E	N	110	6E	n
15	F	[SHIFT IN]	47	2F	/	79	4F	O	111	6F	o
16	10	[DATA LINK ESCAPE]	48	30	0	80	50	P	112	70	p
17	11	[DEVICE CONTROL 1]	49	31	1	81	51	Q	113	71	q
18	12	[DEVICE CONTROL 2]	50	32	2	82	52	R	114	72	r
19	13	[DEVICE CONTROL 3]	51	33	3	83	53	S	115	73	s
20	14	[DEVICE CONTROL 4]	52	34	4	84	54	T	116	74	t
21	15	[NEGATIVE ACKNOWLEDGE]	53	35	5	85	55	U	117	75	u
22	16	[SYNCHRONOUS IDLE]	54	36	6	86	56	V	118	76	v
23	17	[END OF TRANS. BLOCK]	55	37	7	87	57	W	119	77	w
24	18	[CANCEL]	56	38	8	88	58	X	120	78	x
25	19	[END OF MEDIUM]	57	39	9	89	59	Y	121	79	y
26	1A	[SUBSTITUTE]	58	3A	:	90	5A	Z	122	7A	z
27	1B	[ESCAPE]	59	3B	;	91	5B	[	123	7B	{
28	1C	[FILE SEPARATOR]	60	3C	<	92	5C	\	124	7C	|
29	1D	[GROUP SEPARATOR]	61	3D	=	93	5D	]	125	7D	}
30	1E	[RECORD SEPARATOR]	62	3E	>	94	5E	^	126	7E	~
31	1F	[UNIT SEPARATOR]	63	3F	?	95	5F	_	127	7F	[DEL]

Figure 5. 16: (ASCII Table. Source: sciencebuddies.org, 7 September 2023)

Table 5.6 shows the information of the user and the device, the ASCII value of the information, and the encryption value of the information. The encryption is calculated using the formula below.

$$y = x^e \ mod \ n$$

(Equation 5. 8): The encryption value, y.

Table 5. 6: Information of the User and Device, the ASCII Value, and the Encrypted Value for the First Simulated Data.

Information	User (U)	Device (D)
UserID / IMEI number	test	3584
ASCII Value	116 101 115 116	51 53 56 52
Encrypted value, y	08 29 25 08	86 32 56 03

Based on the formula 5.8 above, to calculate the value of encrypted value y, the steps are as below:

For the user's ASCII value: $y = 116^7 \ mod\ 33 = 08$

(Equation 5. 9): User's ASCII value, y.

For device's ASCII value: $y = 51^7 \ mod\ 133 = 86$

(Equation 5. 10): Device's ASCII value, y.

The signature value based on the encrypted value above is calculated using formula 1.16 below. Note that the researcher has compiled the userID followed by the IMEI number as a string of information whereas the device has compiled the IMEI number followed by UserID as a string of information. To sign the encrypted user and device information, the formula used is shown below.

$$s = y^d \ mod\ n$$

(Equation 5. 11): Digital Signature to sign encrypted user and device value, s.

For the verification of the signature, the formula used is shown below.

$$x' = s^e \ mod \ n$$

(Equation 5. 12): verification of the signature, x'.

The private key, d, public key exponential, e, and the value n were obtained from the CA's n value, private key and public key which are 143, 43 and 7 respectively.

The calculation below shows the signature value, s, and verification value, x' for encrypted value, y is calculated using the following equations 5.13 and 5.14 below.

$$s = \ 8^{43} \ mod \ 143 = 83$$

(Equation 5. 13): Signature value, s.

$$x' = 83^7 \ mod \ 143 = 8$$

(Equation 5. 14): Verification value, x'.

The signature of the encrypted information for the user device is shown in Table 5.7.

Table 5. 7: Signature of the Encrypted Value and the Verification Value of the Signature for the First Simulated Data.

Information	User	Device
Encrypted value, y	08 29 25 08 86 32 56 03	86 32 56 03 08 29 25 08
Signature Value, s	83 68 38 83 135 98 56 16	135 98 56 16 83 68 38 83
Verification Value, x'	08 29 25 08 86 32 56 03	86 32 56 03 08 29 25 08

From Table 5.7 above, we can observe that the Verification Value, x' is similar to the encrypted value, y. Thus, this proves that the authentication is correct and both the user and the device are allowed to log in to the system.

5.7.2 Simulated Data Two

The second simulation data is used to emphasize the effectiveness of the proposed User-Device Model with Digital Certificate for Smartphone user. Table 5.8 below shows the value of p, q, n, Φ(n), e and d for user, device and certificate authority (CA) respectively for the second stimulation data.

Table 5. 8: Value of p and q for User, Device, and CA for Second Simulated Data.

Prime value	User (U)	Device (D)	Certificate Authority (CA)
p	13	17	19
q	7	11	17
n	91	187	323
Φ(n),	72	160	288
Public key (n,e)	(91,17)	(187,97)	(323,7)
Private key (n,d)	(91,5)	(187,33)	(323,103)

The second simulated date chosen for UserID is '*book*' and the device IMEI number is 3692. These two pieces of information need to be converted to decimal value using the ASCII Table shown in Figure 5.16. The word 'rest' is converted to 98 111 111 107 and the IMEI number 3692 is converted to 51 56 57 50. These values must be encrypted using the public key of the user and device respectively. The calculation is done using Omni Calculator.

Table 5.9 shows the information of the user and the device, the ASCII value of the information, and the encryption value of the information. The encryption is calculated using the formula from 1.15 above.

For the user's ASCII value: $y = 98^{17} \ mod \ 91 = 63$

(Equation 5. 15): User's ASCII value, y.

For device's ASCII value: $y = 51^{97} \ mod \ 187 = 17$

(Equation 5. 16): Device's ASCII value, y.

Table 5. 9: Information of the User and Device, the ASCII Value, and the Encrypted Value for the Second Simulated Data.

Information	User (U)	Device (D)
UserID / IMEI number	book	3692
ASCII Value	98 111 111 107	51 56 57 50
Encrypted value, y	63 76 76 74	17 56 40 118

The signature value based on the encrypted value above is calculated using formula 5.17 below and for the verification of the signature, formula 5.18 below is used. The signature of the encrypted information for the user device is shown in Table 5.10.

$$s = 63^{103} \ mod \ 323 = 194$$

(Equation 5. 17): Signature value, s.

$$x' = 194^{7} \ mod \ 323 = 63$$

(Equation 5. 18): Verification value, x'.

Table 5. 10: Signature of the Encrypted Value and the Verification Value of the Signature for the Second Simulated Data.

Information	User	Device
Encrypted value, y	63 76 76 74 17 56 40 118	17 56 40 118 63 76 76 74

Signature Value, s	194 304 304 320 187 265 269 237	187 265 269 237 194 304 304 320
Verification Value, x'	63 76 76 74 17 56 40 118	17 56 40 118 63 76 76 74

From Table 5.10 above, we can observe that the Verification Value, x' is similar to the encrypted value, y. Thus, this proves that the authentication is correct and both the user and the device are allowed to log in to the system.

5.8 Summary

This research is done using mixed-mode measures. Once the main research contribution which is the design of a User-Device Authentication Model with a Digital Certificate for smartphone user is done, the researcher then drafts questions related to the proposed model. These questionnaires are answered by eight expert reviews that have in-depth knowledge related to authentication and information security once the researcher explains to them the flow of the model. The computation of Cronbach's Alpha indicates that the surveys are reliable, confirming the validity of professional opinions regarding the effectiveness of the suggested authentication methodology. By means of extensive three phases in the proposed authentication model, specialists have furnished answers and suggestions, cultivating assurance about the practicability of executing the suggested model in the sector.

Using two simulated datasets, this research further calculates the expected outcome of the authentication model verification procedure. This proposed authentication model attempts to determine if the anticipated result corresponds with the main goal of the research, which is to verify the simultaneous authentication of the user and device by means of digital certificates as a requirement for system access.

Based on the two datasets shows that both users can be authenticated together using their digital signature. The proposed User-Device Authentication Model for smartphone users is assessed in the thesis using the qualitative technique as it provides in-depth analysis and professional input on the model. The efficacy and security of the suggested model are evaluated in-depth by the research using reviews from experts. Information security experts are asked to assess several parts of the model, such the authentication procedure, certificate issuing, and registration phase. These specialists can offer detailed comments, practical problems, security feature evaluations, and ideas for improvement thanks to the qualitative method. The model needs to be refined with the help of these detailed, comprehensive comments.

The thesis provides mathematical validation of the User-Device Authentication Model through the application of the quantitative technique, especially by the calculation of simulated data. This strategy provides objective, data-driven proof that the model operates as intended, which enhances the qualitative feedback. The suggested model's accuracy in performing cryptographic operations, such as key creation, encryption, and RSA decryption, is confirmed by simulation data. The model's procedures are guaranteed to be mathematically sound and to adhere to accepted cryptography principles by this quantitative examination.

The quantitative calculations verify the validity and expected performance of the authentication procedures (verification, certificate issue, and registration) within the specified limits.