APPENDIX A

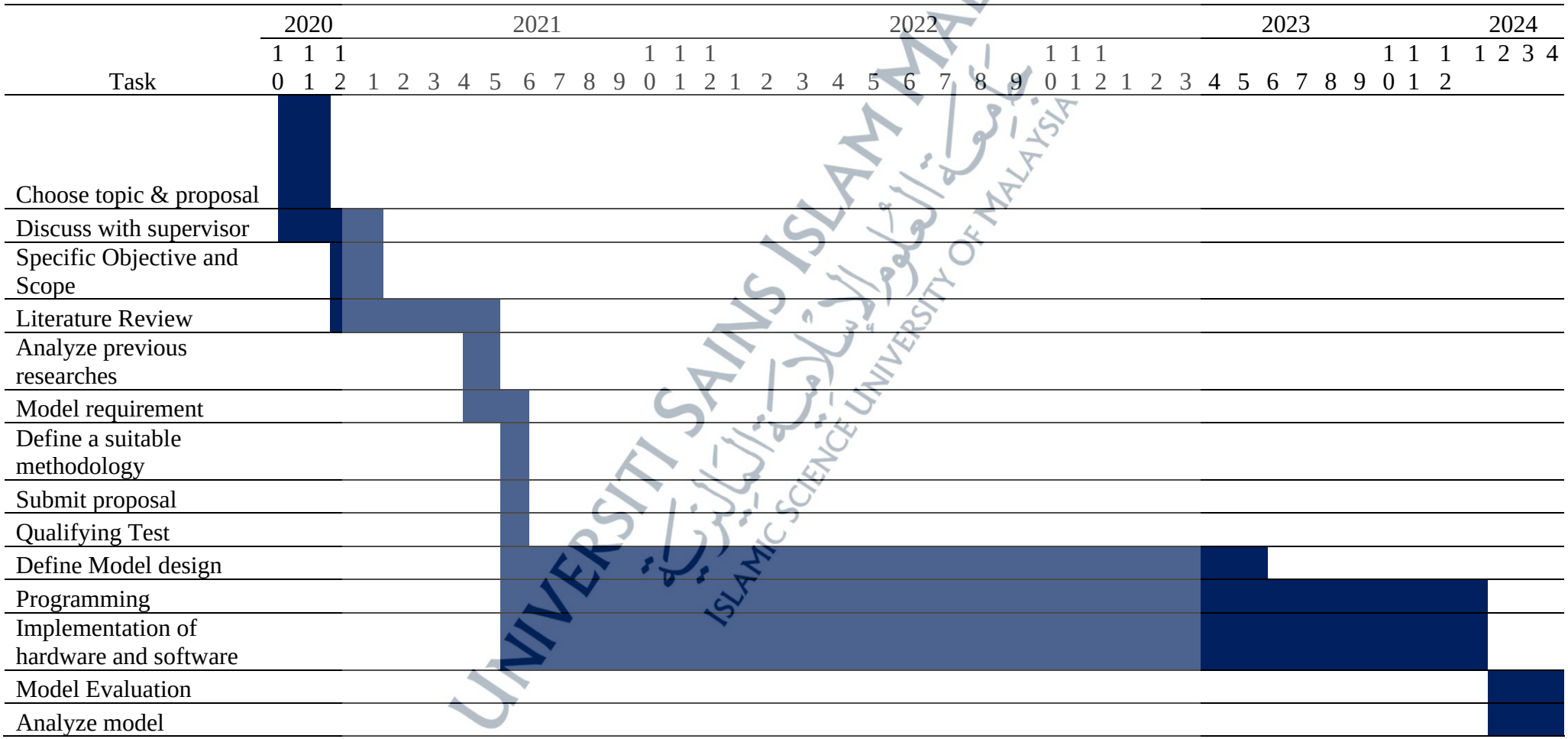
Appendix A: Milestone of the Thesis

Milestone	Research Activity	Start Date	End Date	Deliverable
M1	Choose topic and proposal	19/10/2020	30/10/2020	Choose a thesis topic
	Discuss with supervisor	22/10/2020	10/11/2020	
M2	Specify objective and scope	11/11/2020	25/11/2020	Identify all the requirements of the thesis and important points of the thesis and analyze all the researches related to the system.
	Literature review	26/11/2020	15/2/2021	
	Analyze previous researches	16/2/2021	28/2/2020	
	Model requirement	1/2/2021	3/3/2021	
M3	Define a suitable methodology	4/3/2021	13/3/2021	An efficient method to develop the system
	Submit Proposal	15/3/2021	15/3/2021	Final thesis proposal
	Qualifying Test	22/3/2021	26/3/2021	Proposal approval
M4	Define Model Design	1/4/2021	15/5/2022	The interface of the proposed model

	Algorithm	1/4/2021	23/12/2022	Algorithm implementation in the proposed model
	Implementation of hardware and software	1/4/2021	25/12/2022	
M5	Model Evaluation	1/1/2023	1/4/2023	The proposed model is evaluated using questionnaire
	Analyze model	2/4/2023	15/8/2023	The result shows whether the proposed model is reliable or not
M6	Thesis Writing	1/1/2023	11/4/2024	Softbound copy of a final thesis
	Viva Presentation	11/7/2024	11/7/2024	Thesis poster and a completed of system

APPENDIX B

Appendix B: Gantt Chart



Thesis writing

Submit & present thesis

APPENDIX C

Appendix C: Questionnaires User-Device Authentication Model for Smartphone User

UNIVERSITI SAINS ISLAM MALAYSIA
جَامِعَة العُلوم الإسْلامِيَة المَالِيزِيَة
ISLAMIC SCIENCE UNIVERSITY OF MALAYSIA

Title: User-Device Authentication Model with Digital Certificate for Smartphone User

My name is Sakiinah binti Altaf Hussain (3201278), a Master of Science student at Universiti Sains Islam Malaysia (USIM). I am conducting research entitled **'User-Device Authentication Model with Digital Certificate for Smartphone User'** to meet one of the requirements for a Master of Science.

This questionnaire is comprised of 15 close-ended questions with suggestions for each question. The objective is **to validate the User-Device Authentication Model for for Smartphone User.**

Therefore, your fair assessment and remarks on this model is much appreciated, and we are hoping that with your contribution, this research will be a small step in the bigger efforts to continuously improve the landscape of our education.

All information provided will only be used for the purpose of this research and **will be kept confidential**. It will be stored using electronic storage system.

Thank you for spending your time to complete this questionnaire. Your response is very valuable for the success of this research. If you have any inquiries, please contact me at +6017-4620676 or via email sakiinahaltaf.fst@gmail.com.

Researcher:
Sakiinah binti Altaf Hussain
Email: sakiinahaltaf.fst@gmail.com
Phone No: 017-4620676
Faculty of Science and Technology

Supervisors:
Assoc. Prof Dr. Azni Haslizan Ab. Halim
Assoc. Prof Dr. Najwa Hayaati Mohd Alwi

Section A: About the Evaluator

Name: ……

Job Position/Expertise: ……

Company Name: ……..

Years of Experience: ……

Section B: Questionnaire about the User-Device Authentication Model

Please refer to Appendix A: User-Device Authentication Model with Digital Certificate for Smartphone User and kindly answer all the questions by 'ticking' the box and adding any comment for each question.

The model comprises three phases which are

a) Registration Phase
b) Digital Certificate Issue Phase
c) Authentication/Validation Phase

a) Registration Phase

3. It is more secure to register both the user and the device rather than just registering the user for authentication in smartphone application.

	Strongly Disagree
	Disagree
	Neutral
	Agree
	Strongly Agree

Add Comment:

4. Registering a user's device using the user's phone number and the device's IMEI number fetched from device is more secure for authentication compared to only registering the user's phone number.

	Strongly Disagree
	Disagree
	Neutral
	Agree
	Strongly Agree

Add Comment:

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

	Strongly Disagree
	Disagree
	Neutral
	Agree
	Strongly Agree

Add Comment:

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

	Strongly Disagree
	Disagree
	Neutral
	Agree
	Strongly Agree

Add Comment:

b) Digital Certificate Issue Phase

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

	Strongly Disagree
	Disagree
	Neutral
	Agree
	Strongly Agree

Add Comment:

19. 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).

	Strongly Disagree
	Disagree
	Neutral
	Agree
	Strongly Agree

Add Comment:

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

	Strongly Disagree
	Disagree
	Neutral
	Agree
	Strongly Agree

Add Comment:

21. 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.

	Strongly Disagree
	Disagree
	Neutral
	Agree
	Strongly Agree

Add Comment:

22. 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.

	Strongly Disagree
	Disagree
	Neutral
	Agree
	Strongly Agree

Add Comment:

c) Authentication/Verifying Phase

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

	Strongly Disagree
	Disagree
	Neutral
	Agree
	Strongly Agree

Add Comment:

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

	Strongly Disagree
	Disagree
	Neutral
	Agree
	Strongly Agree

Add Comment:

25. 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.

	Strongly Disagree
	Disagree
	Neutral
	Agree
	Strongly Agree

Add Comment:

General Questions

26. All three phases in the model are sufficient to assure strong authentication for smartphone application.

	Strongly Disagree
	Disagree

	Neutral
	Agree
	Strongly Agree

Add Comment:

27. All the authentication factors which are user, device and Certificate Authority are able to ensure strong authentication for smartphone application.

	Strongly Disagree
	Disagree
	Neutral
	Agree
	Strongly Agree

Add Comment:

28. This model is suitable to be apply in smartphone application.

	Strongly Disagree
	Disagree
	Neutral
	Agree
	Strongly Agree

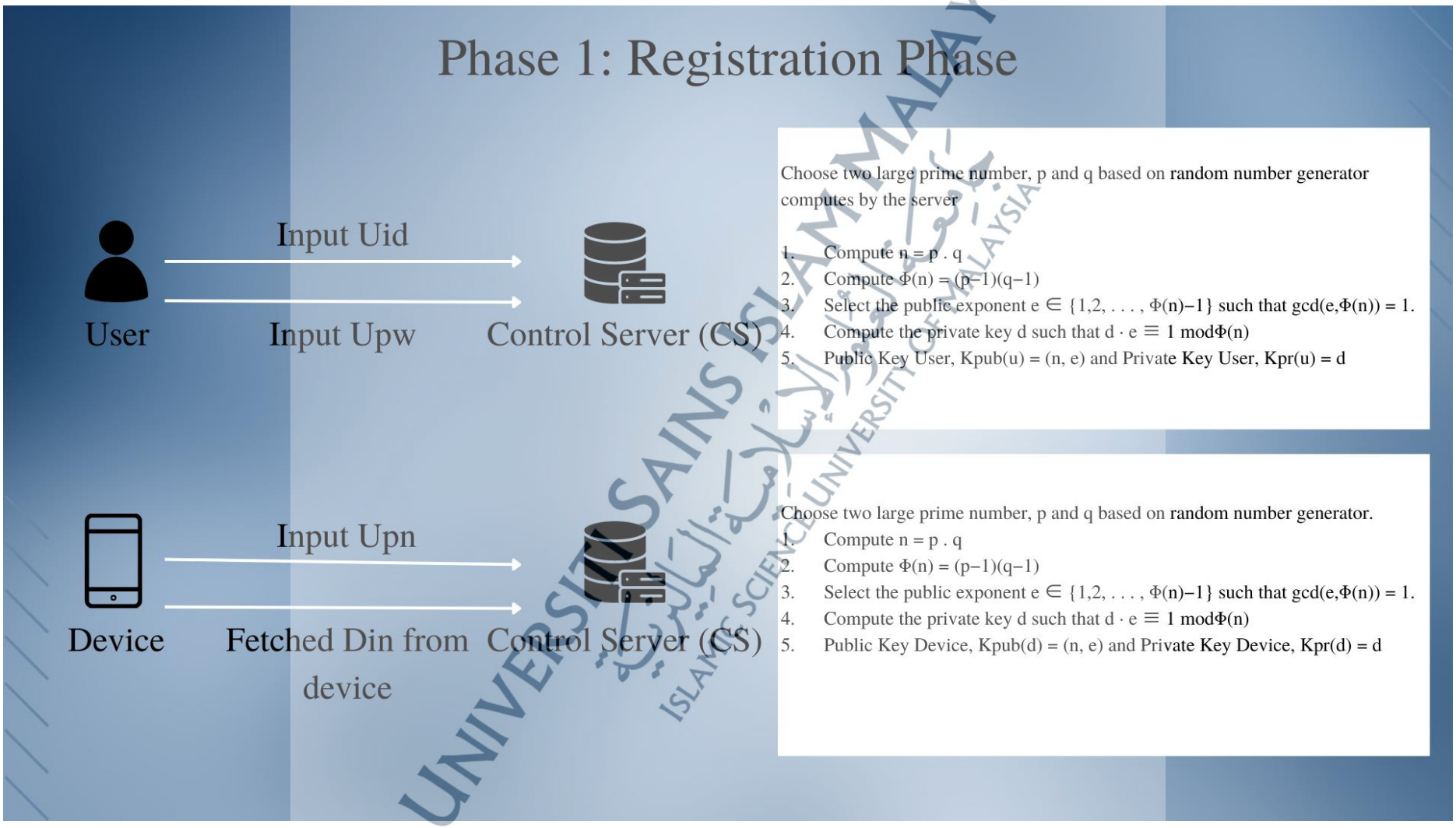
Add Comment:

Answered by:

(Signature)

Name:

Appendix A: User-Device Authentication Model with Digital Certificate for smartphone User.



Registration Phase

Step 1: User will register themselves by keying in their User Identity, Uid, and creating their password, Upw. The Uid and Upw will be stored in the control server, CS.

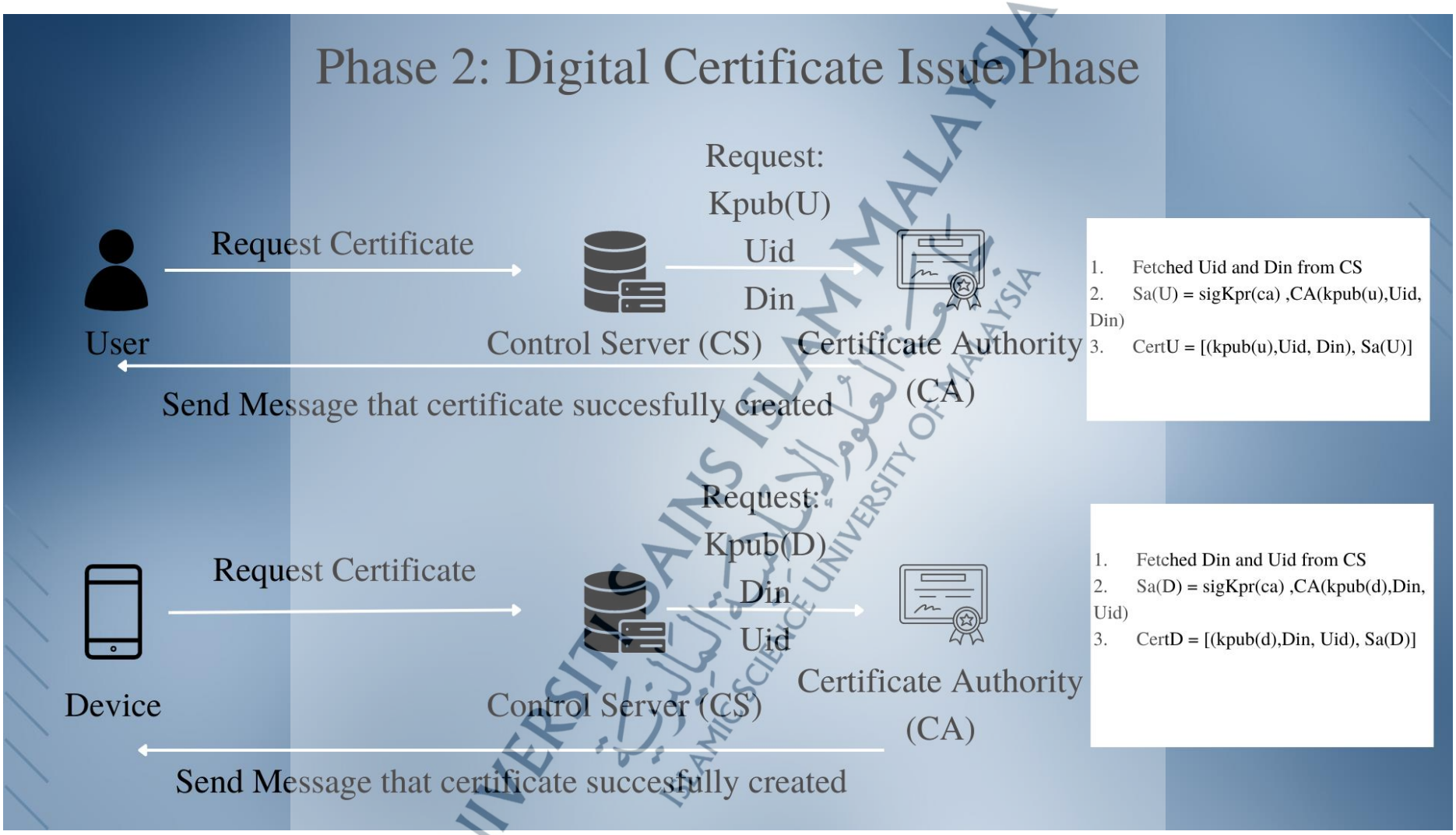
Step 2: The user registers their device by inserting the user's phone number, Upn, and fetched the device's IMEI number, Din, from the device. The Upn and Din will be stored in the control server, CS

Step 3: The Control Server (CS) will compute user's key first by using two large prime numbers, p, and q randomly based on a random number generator. the value n is calculated by multiplying both p and q, thus, $n = p \cdot q$.

Step 4: Calculate Euler's Totient, $\Phi(n) = (p-1)(q-1)$ in order to calculate public exponential, e. Public exponential, e, is select by $e \in \{1,2, \ldots, \Phi(n)-1\}$ such that $\gcd(e,\Phi(n)) = 1$.

Step 5: Compute the private key d such that $d \cdot e \equiv 1 \bmod \Phi(n)$ the Public Key User, Kpub(u) is calculated by Kpub(u) = (n, e) and Private Key User, Kpr(u) = d

Step 6: Step 3 until step 5 is repeated in order to calculate the Public Key and Private key for device depicted Kpub(d) and Kpr(d).



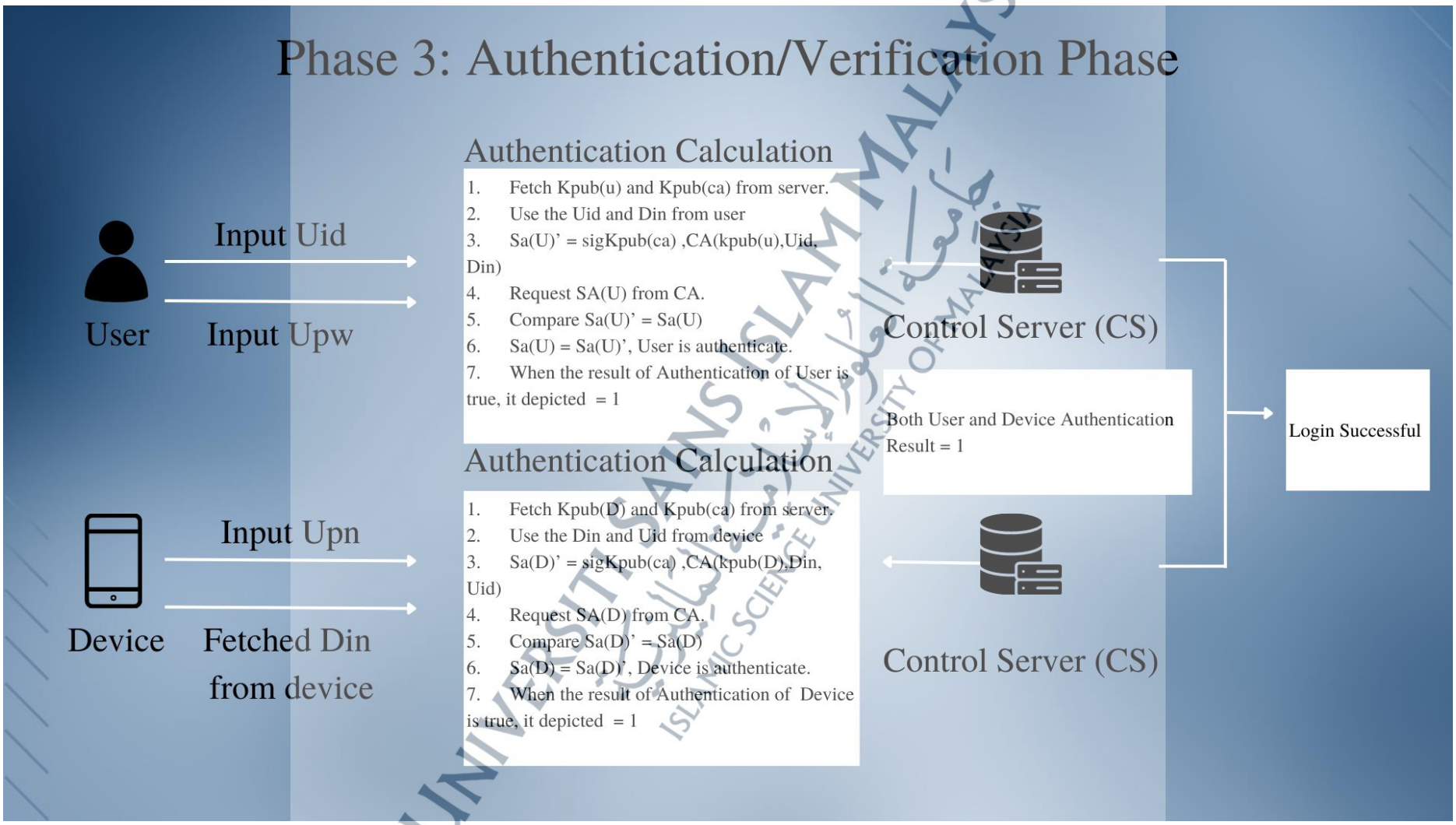
Digital Certificate Issue Phase

Step 7: User will request a digital certificate for themselves and for their device. The Certificate Authority (CA) responsible to issue a certificate will request information regarding the user, which are the user's public key, Kpub(u), user's ID, Uid and User's device IMEI number, Din from the control server (CS).

Step 8: The CA will sign the certificate containing user's information using their own private key, Kpr(ca). The information that CA sign contain in the certificate are the user's public key, Kpub(u), user's ID, Uid and Device's IMEI number, Din.

Step 9: Once the certificate for the user has been issued by CA, the certificate will be stored by CA. A message will be send to the user and device to inform them that their certificate has been successfully created. This certificate need to be renewed every year to maintain the secrecy of user's key.

Step 10: Step 8 and step 9 is repeated again to issue a certificate for the device of the user. The information signed by the CA that contains in the device's certificate are device's Public key, Kpub(d), device's IMEI number, Din and User's ID which has been signed using CA's private key, Kpr(ca).



APPENDIX D

Appendix D: Questionnaire Answered by Expert Reviews

1) Dr. Abdul Alif Zakaria

Researcher:
Sakiinah binti Altaf Hussain
Email: sakiinahaltaf.fst@gmail.com
Phone No: 017-4620676
Faculty of Science and Technology

Supervisors:
Assoc. Prof Dr. Azni Haslizan Ab. Halim
Assoc. Prof Dr. Najwa Hayaati Mohd Alwi

Section A: About the Evaluator

Name: Dr. Abdul Alif Zakaria

Job Position/Expertise: Senior Analyst / Information Security

Company Name: Cyber Security Malaysia

Years of Experience: 13 years

Section B: Questionnaire about the User-Device Authentication Model

Please refer to Appendix A: User-Device Authentication Model with Digital Certificate in IoT Application and kindly answer all the questions by 'ticking' the box and adding any comment for each question.

The model comprises three phases which are

a) Registration Phase
b) Digital Certificate Issue Phase
c) Authentication/Validation Phase

a) Registration Phase

1. It is more secure to register both the user and the device rather than just registering the user for authentication in an IoT application.

	Strongly Disagree
	Disagree
	Neutral
	Agree
✓	Strongly Agree

Add Comment:

2. Registering a user's device using the user's phone number and the device's IMEI number fetched from device is more secure for authentication compared to only registering the user's phone number.

	Strongly Disagree
	Disagree
	Neutral
	Agree
✓	Strongly Agree

Add Comment:

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

	Strongly Disagree
	Disagree
	Neutral
	Agree
✓	Strongly Agree

Add Comment:

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

	Strongly Disagree
	Disagree
	Neutral
	Agree
✓	Strongly Agree

Add Comment:

b) Digital Certificate Issue Phase

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

	Strongly Disagree
	Disagree
	Neutral
	Agree
✓	Strongly Agree

Add Comment:

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).

~~✓~~	Strongly Disagree
	Disagree
	Neutral
	Agree
✓	Strongly Agree

Add Comment:

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

~~✓~~	Strongly Disagree
	Disagree
	Neutral
	Agree
✓	Strongly Agree

Add Comment:

8. 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.

	Strongly Disagree
	Disagree
	Neutral
✓	Agree
	Strongly Agree

Add Comment: ... CA to generate a new certificate provided the user generated a new key pair.

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.

	Strongly Disagree
	Disagree
	Neutral
	Agree
✓	Strongly Agree

Add Comment:

c) Authentication/Verifying Phase

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

	Strongly Disagree
	Disagree
	Neutral
	Agree
✓	Strongly Agree

Add Comment:

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

	Strongly Disagree
	Disagree
	Neutral
	Agree
✓	Strongly Agree

Add Comment:

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.

	Strongly Disagree
	Disagree
	Neutral
	Agree
✓	Strongly Agree

Add Comment:

General Questions

13. All three phases in the model is sufficient to assure strong authentication for IoT application.

	Strongly Disagree
	Disagree
	Neutral
	Agree
✓	Strongly Agree

Add Comment:

14. All the authentication factors which are user, device and Certificate Authority are able to ensure strong authentication for IoT application.

	Strongly Disagree
	Disagree
	Neutral
	Agree
✓	Strongly Agree

Add Comment:

15. This model is suitable to be apply in IoT application.

	Strongly Disagree
	Disagree
	Neutral
	Agree
✓	Strongly Agree

Add Comment:

Answered by:

(Signature)

Name: Dr. Abdul Afiq Zakaria

2) Dr. Nur Hafiza Zakaria

Section A: About the Evaluator

Please state your name, job position or expertise, company and and years of experience.

All information provided will only be used for the purpose of this research and will be kept confidential.

Name *

NUR HAFIZA ZAKARIA

Job Position/Expertise *

SENIOR LECTURER

Company Name *

USIM

Years of Experience *

5 YEARS

1. It is more secure to register both the user and the device rather than just registering the user for authentication in smartphone application. *

- (●) Strongly Agree
- ( ) Agree
- ( ) Neutral
- ( ) Disagree
- ( ) Strongly Disagree

Add Comment for Question 1

2. Registering a user's device using the user's phone number and the device's IMEI number fetched from device is more secure for authentication compared to only registering the user's phone number. *

- (●) Strongly Agree
- ( ) Agree
- ( ) Neutral
- ( ) Disagree
- ( ) Strongly Disagree

Add comment for Question 2

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

- ( ) Strongly Agree
- (●) Agree
- ( ) Neutral
- ( ) Disagree
- ( ) Strongly Disagree

Add Comment for Question 3

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

- (●) Strongly Agree
- ( ) Agree
- ( ) Neutral
- ( ) Disagree
- ( ) Strongly Disagree

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

- (●) Strongly Agree
- ( ) Agree
- ( ) Neutral
- ( ) Disagree
- ( ) Strongly Disagree

Add Comment for Question 5

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). *

- ( ) Strongly Agree
- (●) Agree
- ( ) Neutral
- ( ) Disagree
- ( ) Strongly Disagree

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

- (●) Strongly Agree
- ( ) Agree
- ( ) Neutral
- ( ) Disagree
- ( ) Strongly Disagree

Add Comment for Question 7

8. 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. *

- ( ) Strongly Agree
- (●) Agree
- ( ) Neutral
- ( ) Disagree
- ( ) Strongly Disagree

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. *

- (●) Strongly Agree
- ( ) Agree
- ( ) Neutral
- ( ) Disagree
- ( ) Strongly Disagree

10. Double authentication using user and device signature is more secure compare to single authentication for smartphone applications. *

- (●) Strongly Agree
- ( ) Agree
- ( ) Neutral
- ( ) Disagree
- ( ) Strongly Disagree

Add Comment for Question 10

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

- (●) Strongly Agree
- ( ) Agree
- ( ) Neutral
- ( ) Disagree
- ( ) Strongly Disagree

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. *

- ( ) Strongly Agree
- (●) Agree
- ( ) Neutral
- ( ) Disagree
- ( ) Strongly Disagree

13. All three phases in the model is sufficient to assure strong authentication for smartphone application. *

- (●) Strongly Agree
- ( ) Agree
- ( ) Neutral
- ( ) Disagree
- ( ) Strongly Disagree

14. All the authentication factors which are user, device and Certificate Authority are able to ensure strong authentication for smartphone application. *

- (●) Strongly Agree
- ( ) Agree
- ( ) Neutral
- ( ) Disagree
- ( ) Strongly Disagree

Add Comment for Question 14

15. This model is suitable to be apply in smartphone application. *

- (●) Strongly Agree
- ( ) Agree
- ( ) Neutral
- ( ) Disagree
- ( ) Strongly Disagree

3) Dr. Noorul Halimin Binti Mansul

Section A: About the Evaluator
Please state your name, job position or expertise, company and and years of experience.

All information provided will only be used for the purpose of this research and will be kept confidential.

Name *

Noorul Halimin Binti Mansol

Job Position/Expertise *

Freelance Auditor

Company Name *

SIRIM QAS Sdn. Bhd.

Years of Experience *

23

1. It is more secure to register both the user and the device rather than just registering the user for authentication in smartphone application. *

- (●) Strongly Agree
- ( ) Agree
- ( ) Neutral
- ( ) Disagree
- ( ) Strongly Disagree

2. Registering a user's device using the user's phone number and the device's IMEI number fetched from device is more secure for authentication compared to only registering the user's phone number. *

- ( ) Strongly Agree
- (●) Agree
- ( ) Neutral
- ( ) Disagree
- ( ) Strongly Disagree

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

- ○ Strongly Agree
- ◉ Agree
- ○ Neutral
- ○ Disagree
- ○ Strongly Disagree

Add Comment for Question 3

Please consider to propose use Elliptic Curve Cryptography (ECC) also for mobile use.

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

- ○ Strongly Agree
- ◉ Agree
- ○ Neutral
- ○ Disagree
- ○ Strongly Disagree

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

- ○ Strongly Agree
- ◉ Agree
- ○ Neutral
- ○ Disagree
- ○ Strongly Disagree

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). *

- ○ Strongly Agree
- ◉ Agree
- ○ Neutral
- ○ Disagree
- ○ Strongly Disagree

Add Comment for Question 6

To my knowledge, by using email user (during registration phase) this is very low assurance of digital certificate. Pls consider to propose the high level of assurance by using NRIC/passport number to create user ID.

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

- ○ Strongly Agree
- ◉ Agree
- ○ Neutral
- ○ Disagree
- ○ Strongly Disagree

8. 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. *

- ○ Strongly Agree
- ◉ Agree
- ○ Neutral
- ○ Disagree
- ○ Strongly Disagree

Add Comment for Question 8

You may consider to propose the short term validity certificate where the certificate will be purged once been used.

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. *

- ○ Strongly Agree
- ◉ Agree
- ○ Neutral
- ○ Disagree
- ○ Strongly Disagree

10. Double authentication using user and device signature is more secure compare to single authentication for smartphone applications. *

- ○ Strongly Agree
- ◉ Agree
- ○ Neutral
- ○ Disagree
- ○ Strongly Disagree

Add Comment for Question 10

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

- ○ Strongly Agree
- ◉ Agree
- ○ Neutral
- ○ Disagree
- ○ Strongly Disagree

Add Comment for Question 11

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. *

- ○ Strongly Agree
- ◉ Agree
- ○ Neutral
- ○ Disagree
- ○ Strongly Disagree

Add Comment for Question 12

To consider on the time taken for the verification process for example verification with CRLs.

General Questions

13. All three phases in the model is sufficient to assure strong authentication for smartphone application. *

- ○ Strongly Agree
- ◉ Agree
- ○ Neutral
- ○ Disagree
- ○ Strongly Disagree

14. All the authentication factors which are user, device and Certificate Authority are able to ensure strong authentication for smartphone application. *

- ○ Strongly Agree
- ◉ Agree
- ○ Neutral
- ○ Disagree
- ○ Strongly Disagree

15. This model is suitable to be apply in smartphone application. *

- ○ Strongly Agree
- ◉ Agree
- ○ Neutral
- ○ Disagree
- ○ Strongly Disagree

4) Dr. Azuan bin Ahmad

Name *

Dr Azuan Ahmad

Job Position/Expertise *

Lecturer

Company Name *

USIM

Years of Experience *

5

1. It is more secure to register both the user and the device rather than just registering the user for authentication in smartphone application. *

- ◉ Strongly Agree
- ○ Agree
- ○ Neutral
- ○ Disagree
- ○ Strongly Disagree

Add Comment for Question 1

Registering device and user ensure the authencity of the user by requiring both user and device available at the same time

2. Registering a user's device using the user's phone number and the device's IMEI number fetched from device is more secure for authentication compared to only registering the user's phone number. *

- (●) Strongly Agree
- ( ) Agree
- ( ) Neutral
- ( ) Disagree
- ( ) Strongly Disagree

Add comment for Question 2

IMEI is unique identifier for each mobile pjone while phone number can be clone or use at different device

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

- (●) Strongly Agree
- ( ) Agree
- ( ) Neutral
- ( ) Disagree
- ( ) Strongly Disagree

Add Comment for Question 3

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

- (●) Strongly Agree
- ( ) Agree
- ( ) Neutral
- ( ) Disagree
- ( ) Strongly Disagree

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

- (●) Strongly Agree
- ( ) Agree
- ( ) Neutral
- ( ) Disagree
- ( ) Strongly Disagree

Add Comment for Question 5

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). *

- (●) Strongly Agree
- ( ) Agree
- ( ) Neutral
- ( ) Disagree
- ( ) Strongly Disagree

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

- (●) Strongly Agree
- ( ) Agree
- ( ) Neutral
- ( ) Disagree
- ( ) Strongly Disagree

8. 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. *

- ○ Strongly Agree
- ◉ Agree
- ○ Neutral
- ○ Disagree
- ○ Strongly Disagree

Add Comment for Question 8

But in practise it will incured some cost for the user

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. *

- ○ Strongly Agree
- ◉ Agree
- ○ Neutral
- ○ Disagree
- ○ Strongly Disagree

Add Comment for Question 9

10. Double authentication using user and device signature is more secure compare to single authentication for smartphone applications. *

- ◉ Strongly Agree
- ○ Agree
- ○ Neutral
- ○ Disagree
- ○ Strongly Disagree

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

- (●) Strongly Agree
- ( ) Agree
- ( ) Neutral
- ( ) Disagree
- ( ) Strongly Disagree

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. *

- (●) Strongly Agree
- ( ) Agree
- ( ) Neutral
- ( ) Disagree
- ( ) Strongly Disagree

Add Comment for Question 12

General Questions

13. All three phases in the model is sufficient to assure strong authentication for smartphone application. *

- (●) Strongly Agree
- ( ) Agree
- ( ) Neutral
- ( ) Disagree
- ( ) Strongly Disagree

14. All the authentication factors which are user, device and Certificate Authority are able to ensure strong authentication for smartphone application. *

- (●) Strongly Agree
- ( ) Agree
- ( ) Neutral
- ( ) Disagree
- ( ) Strongly Disagree

Add Comment for Question 14

15. This model is suitable to be apply in smartphone application. *

- ( ) Strongly Agree
- (●) Agree
- ( ) Neutral
- ( ) Disagree
- ( ) Strongly Disagree

Add Comment for Question 15

Need to consider the user friendliness or may includes additional authentication mechanism in case the user lost their phone

5) Mr. Akhmal Marsidi

Name *

Akhmal Marsidi

Job Position/Expertise *

IT Sec Arch

Company Name *

Orsted Malaysia

Years of Experience *

27

1. It is more secure to register both the user and the device rather than just registering the user for authentication in smartphone application. *

- ○ Strongly Agree
- ◉ Agree
- ○ Neutral
- ○ Disagree
- ○ Strongly Disagree

Add Comment for Question 1

2FA is more secure compares to single factor authentication i.e password only

2. Registering a user's device using the user's phone number and the device's IMEI number fetched from device is more secure for authentication compared to only registering the user's phone number. *

- ○ Strongly Agree
- ◉ Agree
- ○ Neutral
- ○ Disagree
- ○ Strongly Disagree

Add comment for Question 2

Same as #1

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

- ○ Strongly Agree
- ○ Agree
- ◉ Neutral
- ○ Disagree
- ○ Strongly Disagree

Add Comment for Question 3

ECC seems to be more efficient than RSA but RSA is more popular.

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

- ○ Strongly Agree
- ◉ Agree
- ○ Neutral
- ○ Disagree
- ○ Strongly Disagree

Add Comment for Question 4

Private keys need to be with user. CA should only process user's CSR (certificate request). Disagree with CA to generate keypair for users. Btw keypair can be used for different function i.e one for data encryption and the other keypair for digital signature. Single keypair can be used for data encryption & digital signature as well.

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

- ○ Strongly Agree
- ◉ Agree
- ○ Neutral
- ○ Disagree
- ○ Strongly Disagree

Add Comment for Question 5

Agree. One to authenticate user, the other one to authenticate device

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). *

- ○ Strongly Agree
- ◉ Agree
- ○ Neutral
- ○ Disagree
- ○ Strongly Disagree

Add Comment for Question 6

Then both cert have the same info. Using any of the certs will lead to the same object (user with device)

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

- ○ Strongly Agree
- ◉ Agree
- ○ Neutral
- ○ Disagree
- ○ Strongly Disagree

Add Comment for Question 7

Provided the apps should be able to verify/link both users and device are authenticated using their own digital cert . i.e., 'cert-user AND cert-device' instead of 'cert-user OR cert-device' to allow access

8. 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. *

- ○ Strongly Agree
- ○ Agree
- ◉ Neutral
- ○ Disagree
- ○ Strongly Disagree

Add Comment for Question 8

Is the keypair generated automatically as well? Who regenerate the keypair? CA typically process certificate request from user/device and then generate digital signature.

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. *

- ○ Strongly Agree
- ◉ Agree
- ○ Neutral
- ○ Disagree
- ○ Strongly Disagree

Add Comment for Question 9

Provided that private key are stored with user

10. Double authentication using user and device signature is more secure compare to single authentication for smartphone applications. *

- ○ Strongly Agree
- ◉ Agree
- ○ Neutral
- ○ Disagree
- ○ Strongly Disagree

Add Comment for Question 10

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

- ○ Strongly Agree
- ○ Agree
- ◉ Neutral
- ○ Disagree
- ○ Strongly Disagree

Add Comment for Question 11

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. *

- ○ Strongly Agree
- ◉ Agree
- ○ Neutral
- ○ Disagree
- ○ Strongly Disagree

Add Comment for Question 12

With boolen:
Allow only with Certuser AND certdevice

General Questions

13. All three phases in the model is sufficient to assure strong authentication for smartphone application. *

- ○ Strongly Agree
- ○ Agree
- ◉ Neutral
- ○ Disagree
- ○ Strongly Disagree

Add Comment for Question 13

Private key should be with user and never with CA

14. All the authentication factors which are user, device and Certificate Authority are able to ensure strong authentication for smartphone application. *

- ○ Strongly Agree
- ◉ Agree
- ○ Neutral
- ○ Disagree
- ○ Strongly Disagree

Add Comment for Question 14

With correct implementation and private key with user

15. This model is suitable to be apply in smartphone application. *

- ○ Strongly Agree
- ◉ Agree
- ○ Neutral
- ○ Disagree
- ○ Strongly Disagree

Add Comment for Question 15

With correct implementation and private key with user

6) Ms. Nur Syafiqah Mohd Shamsuddin

Name *

Nur Syafiqah Mohd Shamsuddin

Job Position/Expertise *

Digital Forensics Quality Assurance and Analyst

Company Name *

Malaysian Communications and Multimedia Commission (MCMC)

Years of Experience *

4 years

1. It is more secure to register both the user and the device rather than just registering the user for authentication in smartphone application.

- (●) Strongly Agree
- ( ) Agree
- ( ) Neutral
- ( ) Disagree
- ( ) Strongly Disagree

2. Registering a user's device using the user's phone number and the device's IMEI number fetched from device is more secure for authentication compared to only registering the user's phone number. *

- (●) Strongly Agree
- ( ) Agree
- ( ) Neutral
- ( ) Disagree
- ( ) Strongly Disagree

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

- ( ) Strongly Agree
- ( ) Agree
- (●) Neutral
- ( ) Disagree
- ( ) Strongly Disagree

Add Comment for Question 3

Performance shall be considered

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

- ○ Strongly Agree
- ◉ Agree
- ○ Neutral
- ○ Disagree
- ○ Strongly Disagree

Add Comment for Question 4

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

- ○ Strongly Agree
- ◉ Agree
- ○ Neutral
- ○ Disagree
- ○ Strongly Disagree

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). *

- ○ Strongly Agree
- ◉ Agree
- ○ Neutral
- ○ Disagree
- ○ Strongly Disagree

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

- ○ Strongly Agree
- ○ Agree
- ◉ Neutral
- ○ Disagree
- ○ Strongly Disagree

Add Comment for Question 7

Performance of the application in smartphone might differ

8. 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. *

- ○ Strongly Agree
- ◉ Agree
- ○ Neutral
- ○ Disagree
- ○ Strongly Disagree

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. *

- ○ Strongly Agree
- ◉ Agree
- ○ Neutral
- ○ Disagree
- ○ Strongly Disagree

10. Double authentication using user and device signature is more secure compare to single authentication for smartphone applications. *

- ○ Strongly Agree
- ◉ Agree
- ○ Neutral
- ○ Disagree
- ○ Strongly Disagree

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

- ○ Strongly Agree
- ◉ Agree
- ○ Neutral
- ○ Disagree
- ○ Strongly Disagree

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. *

- ○ Strongly Agree
- ○ Agree
- ◉ Neutral
- ○ Disagree
- ○ Strongly Disagree

Add Comment for Question 12

Either way should contribute same result

13. All three phases in the model is sufficient to assure strong authentication for smartphone application. *

- ( ) Strongly Agree
- (•) Agree
- ( ) Neutral
- ( ) Disagree
- ( ) Strongly Disagree

14. All the authentication factors which are user, device and Certificate Authority are able to ensure strong authentication for smartphone application. *

- ( ) Strongly Agree
- ( ) Agree
- (•) Neutral
- ( ) Disagree
- ( ) Strongly Disagree

Add Comment for Question 14

Until proven secured

15. This model is suitable to be apply in smartphone application. *

- ( ) Strongly Agree
- ( ) Agree
- (•) Neutral
- ( ) Disagree
- ( ) Strongly Disagree

Add Comment for Question 15

Not necessarily to be implemented into smartphone application only, there are alao wide range of other computer application should be implemented using this method.

7) Dr. Iznora Aini Zolkifly

here

Name: Dr.Iznora Aini Zolkifly

Job Position/Expertise: Senior Lecturer / Cybersecurity, Computer Graphics

Company Name: UNITAR International University

Years of Experience: 24

Section B: Questionnaire about the User-Device Authentication Model

Please refer to Appendix A: User-Device Authentication Model with Digital Certificate for Smartphone User and kindly answer all the questions by 'ticking' the box and adding any comment for each question.

The model comprises three phases which are

a) Registration Phase
b) Digital Certificate Issue Phase
c) Authentication/Validation Phase

a) Registration Phase

1. It is more secure to register both the user and the device rather than just registering the user for authentication in smartphone application.

	Strongly Disagree
	Disagree
	Neutral
	Agree
/	Strongly Agree

2. Registering a user's device using the user's phone number and the device's IMEI number fetched from device is more secure for authentication compared to only registering the user's phone number.

	Strongly Disagree
	Disagree
	Neutral
	Agree
/	Strongly Agree

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

	Strongly Disagree
	Disagree
	Neutral
/	Agree
	Strongly Agree

Add Comment:

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. Choose the key length carefully based on the security requirements and the capabilities of the target device.

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

	Strongly Disagree
	Disagree
	Neutral
/	Agree
	Strongly Agree

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

	Strongly Disagree
	Disagree
	Neutral
/	Agree
	Strongly Agree

Add Comment:

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.

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).

	Strongly Disagree
	Disagree
	Neutral
/	Agree
	Strongly Agree

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

	Strongly Disagree
	Disagree
	Neutral
	Agree
/	Strongly Agree

8. 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.

	Strongly Disagree
	Disagree
	Neutral
/	Agree
	Strongly Agree

Add Comment: Implement 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 fully aware to notify the user and administrator when a certificate is about to expire,

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.

	Strongly Disagree
	Disagree
	Neutral
	Agree
/	Strongly Agree

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

	Strongly Disagree
	Disagree
	Neutral
	Agree
/	Strongly Agree

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

	Strongly Disagree
	Disagree
	Neutral
	Agree
/	Strongly Agree

Add Comment: Using the CA's public key can also help to prevent unauthorized access by ensuring that only legitimate users with valid certificates are able to access the system.

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.

	Strongly Disagree
	Disagree
	Neutral
	Agree
/	Strongly Agree

Add Comment: 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.

13. All three phases in the model is sufficient to assure strong authentication for smartphone application.

	Strongly Disagree
	Disagree
	Neutral
	Agree
/	Strongly Agree

14. All the authentication factors which are user, device and Certificate Authority are able to ensure strong authentication for smartphone application.

	Strongly Disagree
	Disagree
	Neutral
	Agree
/	Strongly Agree

15. This model is suitable to be apply in smartphone application.

	Strongly Disagree
	Disagree
	Neutral
	Agree
/	Strongly Agree

Add Comment:

This model is suitable to be apply in smartphone application especially in situations where high security is required.

Answered by:

(Signature)

Name: Dr.Iznora Aini Zolkifly

8) Mr. Mas Hairul Rashidi Alwee

Name: MAS HAIRUL RASYIDI BIN ALWEE

Job Position/Expertise: SOFTWARE DEVELOPER

Company Name: NET BYTE SECURITY

Years of Experience: THREE YEARS

1. It is more secure to register both the user and the device rather than just registering the user for authentication in an IoT application.

	Strongly Disagree
	Disagree
	Neutral
	Agree
/	Strongly Agree

2. Registering a user's device using the user's phone number and the device's IMEI number fetched from device is more secure for authentication compared to only registering the user's phone number.

	Strongly Disagree
	Disagree
	Neutral
	Agree
/	Strongly Agree

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

	Strongly Disagree
	Disagree
	Neutral
	Agree
/	Strongly Agree

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

	Strongly Disagree
	Disagree
	Neutral
/	Agree
	Strongly Agree

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

	Strongly Disagree
	Disagree
	Neutral
/	Agree
	Strongly Agree

Add Comment: What happen if the device is a virtual device ? eg. Emulator, Virtual machine

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).

	Strongly Disagree
	Disagree
	Neutral
	Agree
/	Strongly Agree

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

	Strongly Disagree
	Disagree
	Neutral
/	Agree
	Strongly Agree

8. 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.

	Strongly Disagree
	Disagree
	Neutral
	Agree
/	Strongly Agree

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.

	Strongly Disagree
	Disagree
	Neutral
/	Agree
	Strongly Agree

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

	Strongly Disagree
	Disagree
	Neutral
	Agree
/	Strongly Agree

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

	Strongly Disagree
	Disagree
/	Neutral
	Agree
	Strongly Agree

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.

	Strongly Disagree
	Disagree
	Neutral
	Agree
/	Strongly Agree

13. All three phases in the model is sufficient to assure strong authentication for IoT application.

	Strongly Disagree
	Disagree
	Neutral
	Agree
/	Strongly Agree

14. All the authentication factors which are user, device and Certificate Authority are able to ensure strong authentication for IoT application.

	Strongly Disagree
	Disagree
	Neutral
	Agree
/	Strongly Agree

15. This model is suitable to be apply in IoT application.

	Strongly Disagree
	Disagree
	Neutral
	Agree
/	Strongly Agree

Answered by:

(Signature)

Name: MAS HAIRUL RASYIDI BIN ALWEE