Enhancing Security in Wireless Devices for the American Healthcare System

Team Members: Charles Nguyen, Rino Rajan, Andrew Baker, Miguel Villasmil, Yuchen Zhou

Abstract: The large variety of security mechanisms available for wireless devices makes it difficult to identify the combination that is most cost-effective, secure, and accessible for doctors and patients to use. Our project investigates the various security mechanisms such as biometric scanners, data encryption and mobile Trusted Platform Modules. We will study the advantages/disadvantages of each mechanism and perform trade-off analysis respective to cost, feasibility, energy consumption and satisfying the doctor-patient needs.

Table of Contents

Problem Statement

Why is enhancing wireless security necessary?

In the American Healthcare System today, doctor-patient confidentiality is very important and requires sufficient security measures to protect patient data. For example, if sensitive health information regarding government officials or large stakeholders in the economy were leaked to the public, it could negatively affect political decisions and business transactions. Protection of this information using security is necessary for maintaining the privacy between doctors and patients. In addition to the protection of patient data, enhancing the security in wireless devices deters theft.

Who are the project stakeholders?

The stakeholders of this project are health professionals and patients who use the wireless devices to transmit information. Health professionals are concerned with protection of their database of patient's diagnostics. Patients are concerned with keeping their diagnostics private. Extended stakeholders may be medical military personnel in the field who want to secure their wireless devices.

If successful, what are the potential benefits of this project?

If successful, a combination of security mechanisms will be identified to provide the best cost, security, and performance for wireless device security. Finding the best ratio of these metrics will benefit stakeholders by simplifying the complexity of searching for security mechanisms for their wireless devices.

Use Case Development

Who are the actors?

Health Professional: The doctor who performs diagnostics of the patient for health concerns

Patient: A person consulting the doctor for health diagnostics

Cyber Intruder: A malicious person who tries to access the data being transferred over the network for personal gains

Physical Intruder: A malicious person who tries to access the data by theft of wireless device for personal gains

Network System: The system over which data is transmitted and received. It also includes the contingency protocols

What are the functionalities (use cases) of the system?

Attack Prevention: Security mechanisms that prevent attacks

- **Data Encryption:** scrambling of data transmitted to prevent understanding of data contents
- **Platform Integrity Check:** a process that passively runs in the background and checks for malicious processes

User Authentication: Security mechanisms that validate user before granting access

- **Fingerprint Recognition:** only grants access to users with valid fingerprint
- **Voice Recognition:** only grants access to users with valid voice

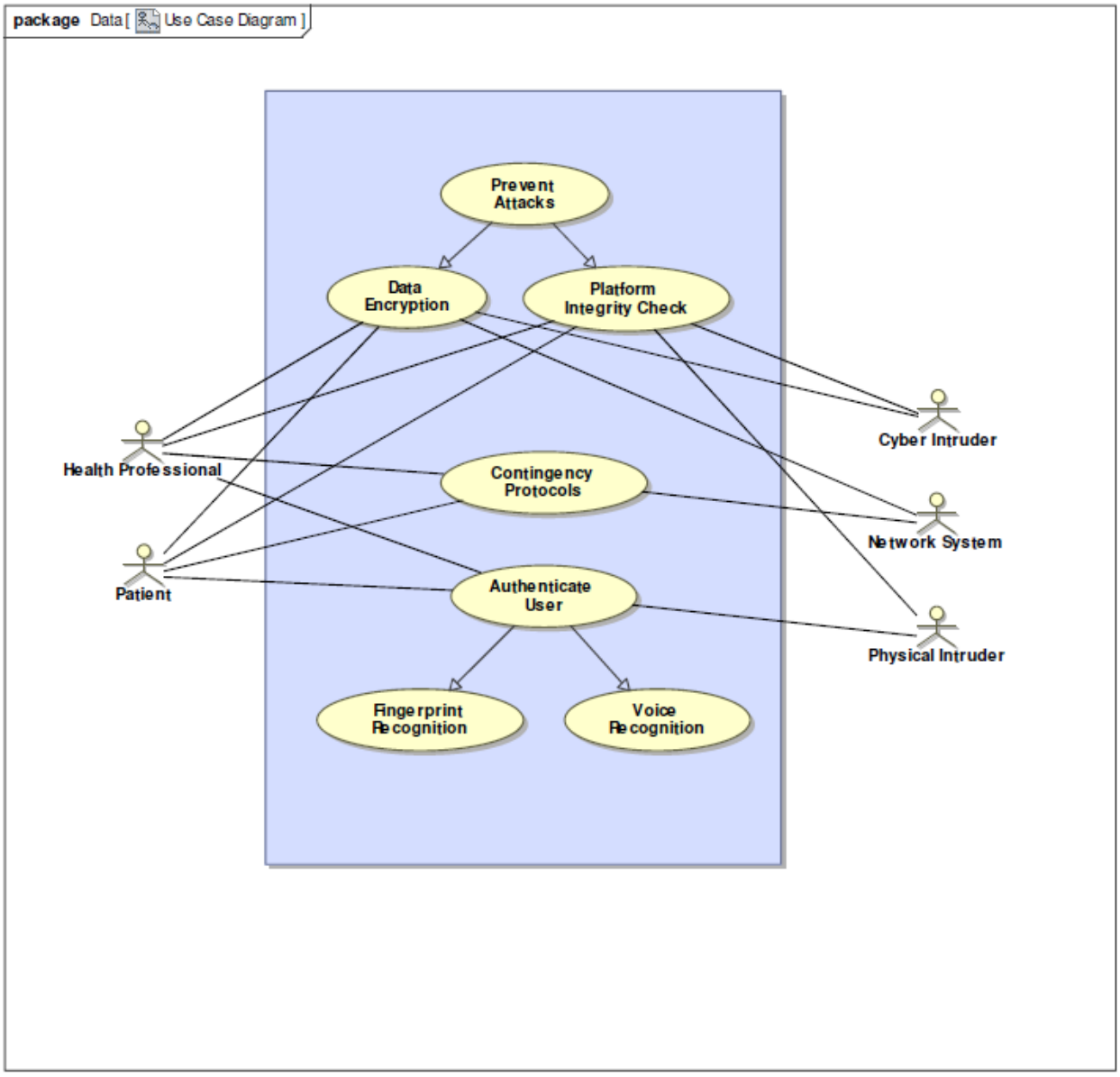
Contingency Protocols: In the event that the patient is incapacitated, congingency protocols can be activated by the health professional to override the security mechanisms on the patients wireless device. This is only used in emergencies when the patient cannot physically unlock their device.

What are the goals of the system?

1. Maintain data security on wireless device
    a. Prevent unauthorized users from physically accessing wireless device
    b. Deny malicious processes from running on wireless device
2. Protect transmission of data to other wireless devices
    a. Prevent unauthorized users from accessing data transmitted from device
3. Maintain authentication reliability
    a. Have high success rates for authorized users
    b. Minimize false positives

What is the relationship between actors and system use cases?

The relationship between actors and system use cases are illustrated in the figure below. The system boundary includes all of the use cases for attack prevention and user authentication. Actors who participate in a system use case are connected via association lines.



Textual Scenarios

Use Case 1: User Authentication – Voice Recognition

Description: Enrolls and verify user voice
Primary Actors: Physical Intruder, Authorized User (Patient, Health Professional)
Pre-conditions: Authorized User is able to speak normally in a suitable environment with minimal background noise.
Flow of Events:

1. Authorized User tries to access the wireless device
2. Device asks for text dependent speaker recognition password
3. Authorized User reads the text to wireless device
4. Device analyzes speech and compares with parameters stored in database
5. Device finds match and grants access to Authorized User

Alternative Flow of Events:

1. Physical Intruder obtains wireless device and tries to access it
2. Device asks for text dependent speaker recognition password
3. Physical Intruder reads text to wireless device
4. Device analyzes speech and compares with parameters stored in database
5. Device does not find match and repeats inquiry for voice input
6. Validation fails 5 attempts and device locks out Physical Intruder

Post-conditions:

Basic Flow: The Authorized User is able to use their wireless device.
Alternative Flow: The Physical Intruder is unable to use their wireless device.

Use Case 2: User Authentication – Fingerprint Recognition

Description: Enrolls and verify user fingerprint
Primary Actors: Physical Intruder, Authorized User (Patient, Health Professional)
Pre-conditions: Authorized User does not have any physical anomalies on their scanning fingers.
Flow of Events:

1. Authorized User tries to access wireless device
2. Device asks for fingerprint swipe
3. Authorized User scans finger
4. Device analyzes swiped fingerprint with fingerprints in database
5. Device finds match and grants access to Authorized User

Alternative Flow of Events:

1. Physical Intruder obtains wireless device and tries to access it
2. Device asks for fingerprint swipe
3. Physical Intruder scans finger
4. Device analyzes swiped fingerprint with fingerprints in database
5. Device does not find match and repeats inquiry for fingerprint
6. Validation fails 5 attempts and device locks out Physical Intruder

Post-conditions:

Basic Flow: The Authorized User is able to use their wireless device.
Alternative Flow: The Physical Intruder is unable to use the wireless device.

Use Case 3: Attack Prevention – Platform Integrity Check

Description: Maintains device integrity
Primary Actors: Physical Intruder, Cyber Intruder, Authorized User (Patient, Health Professional)
Pre-conditions: MTM is operational.
Flow of Events:

1. Intruders get access to wireless device
2. Intruders try to run unauthorized process
3. MTM prevents unauthorized process
4. MTM locks out intruders and notifies Authorized User

Alternate Flow of Events:

None

Post-conditions:

Basic Flow: The Intruders are unable to use the wireless device.

Use Case 4: Attack Prevention – Data Encryption

Description: Encrypt data for secure transmission between devices
Primary Actors: Cyber Intruder, Network System, Authorized User (Patient, Health Professional)
Pre-conditions: Device has network access; data is trying to pass through the firewall.
Flow of Events:

1. Authorized User uses device to transmit data
2. Device uses encryption key to encrypt data using SHA-256
3. Device transmits encrypted data to end user
4. Receiving device receives encrypted data
5. Receiving device retrieves decryption key and decrypts data
6. End user receives and accesses the data

Alternative Flow of Events:

1. Cyber Intruder intercepts encrypted data
2. Cyber Intruder cannot decrypt data
3. Cyber Intruder cannot read data

Post-conditions:

Basic Flow: The Authorized User is able to use their wireless device.
Alternative Flow: The Cyber Intruder is unable to read encrypted data.

Use Case 5: Contingency Protocols

Description: Allow wireless device to transmit patient data to health professional
Primary Actors: Network System, Authorized User (Patient, Health Professional)
Pre-conditions: Device has network access; Patient is incapacitated; Health Professional's wireless device is unlocked.
Flow of Events:

1. Health professional activates contingency protocols
2. Network system bypasses the patients wireless device security mechanisms

3. Patients wireless device automatically transfers data to network system
4. Network system receives data from patients wireless devices
5. Network system transmits patient data to health professional

Alternative Flow of Events:

None

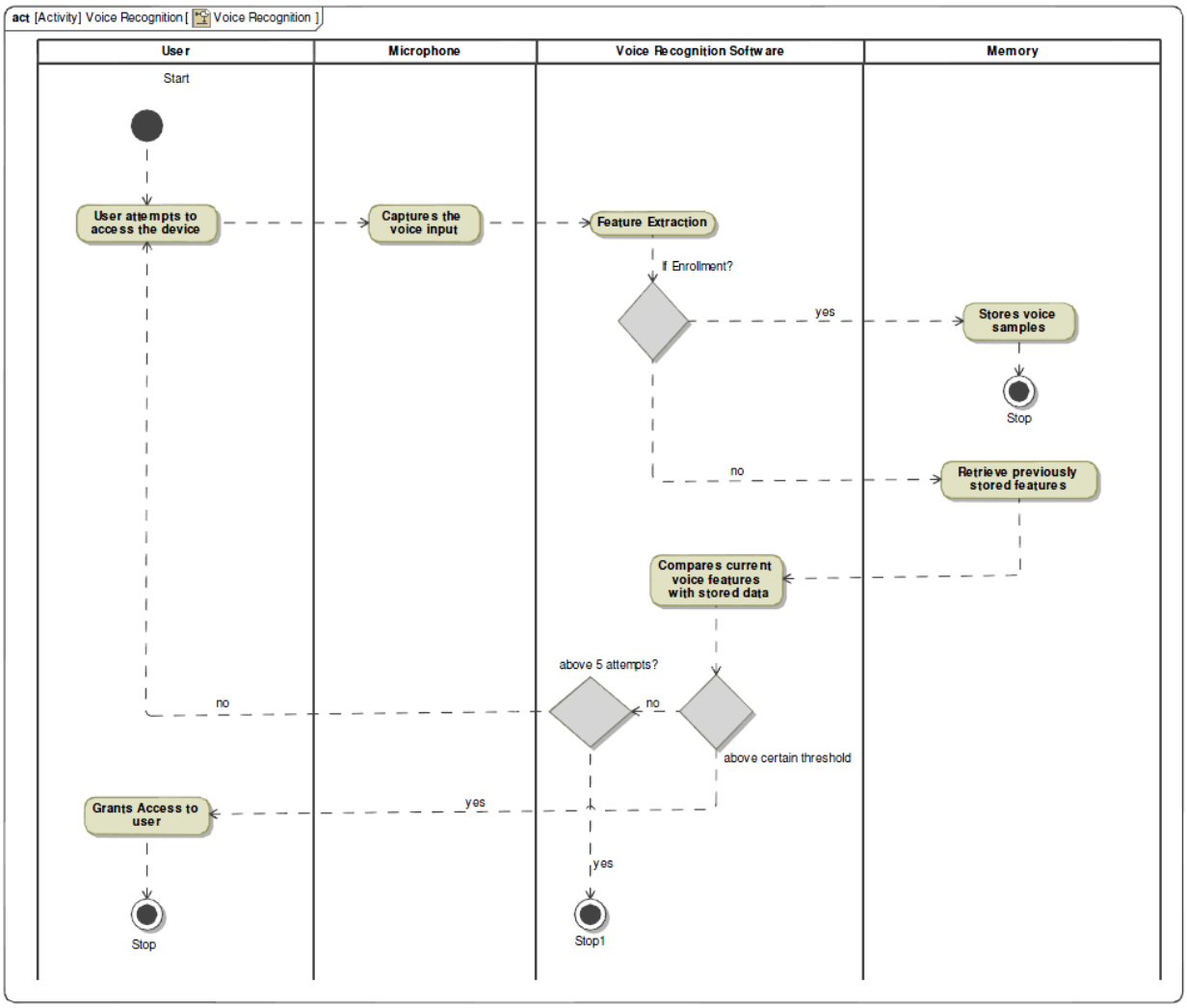
Post-conditions:

Basic Flow: The Health Professional retrieves incapacitated patients data to perform diagnostics.

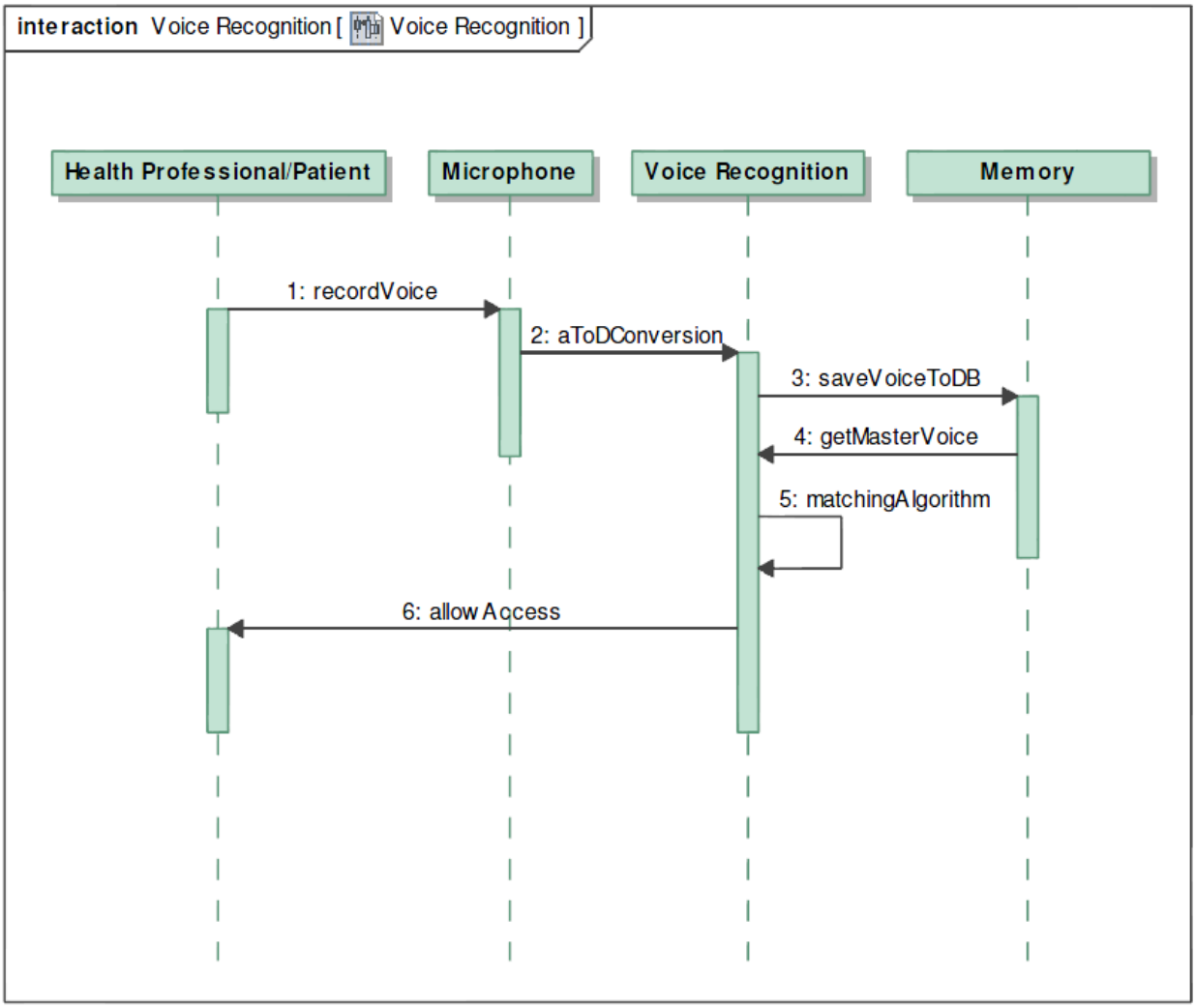
Simplified Models of System Behavior

Voice Recognition Behavior

Voice Recognition Activity Diagram

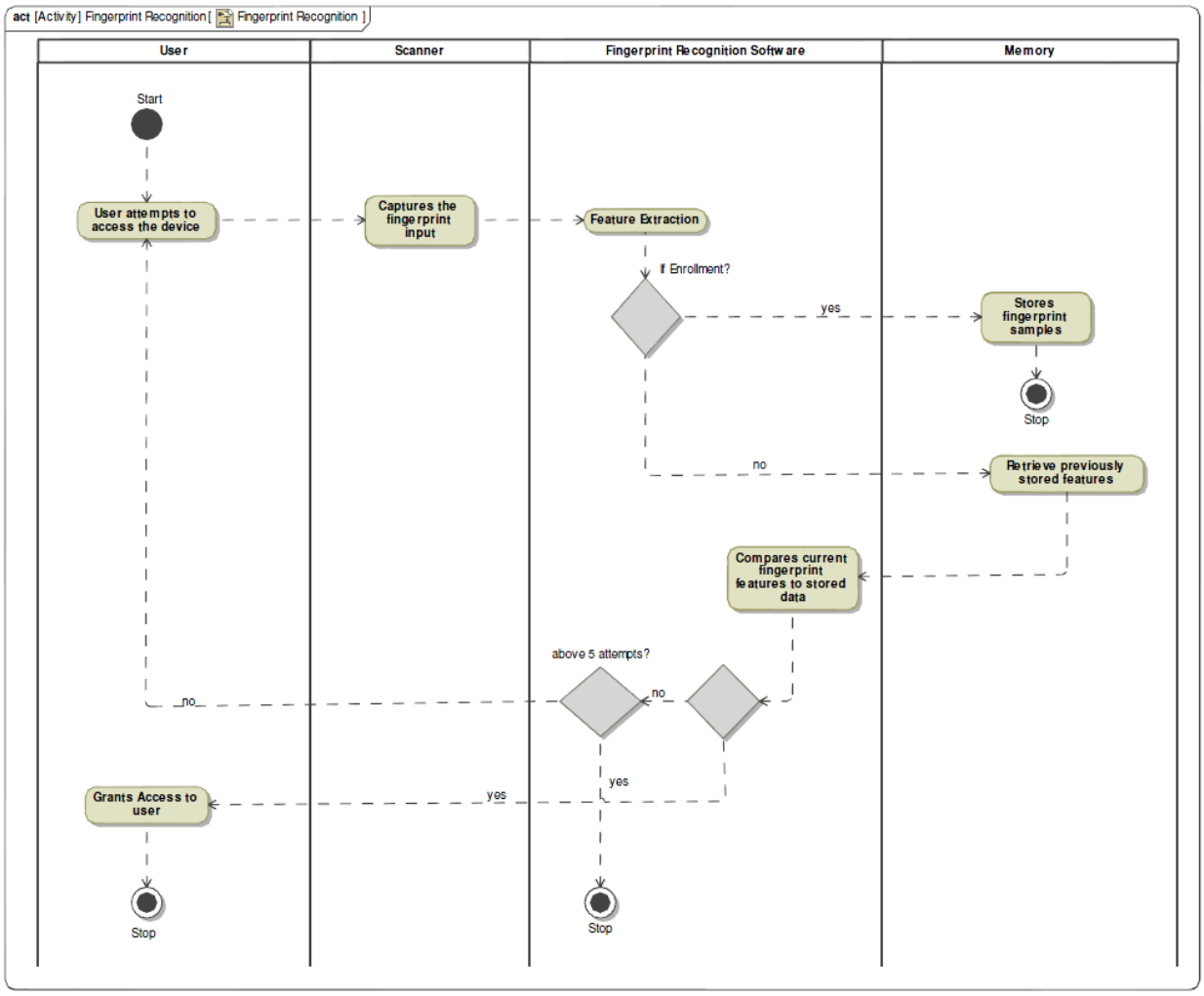


Voice Recognition Sequence Diagram

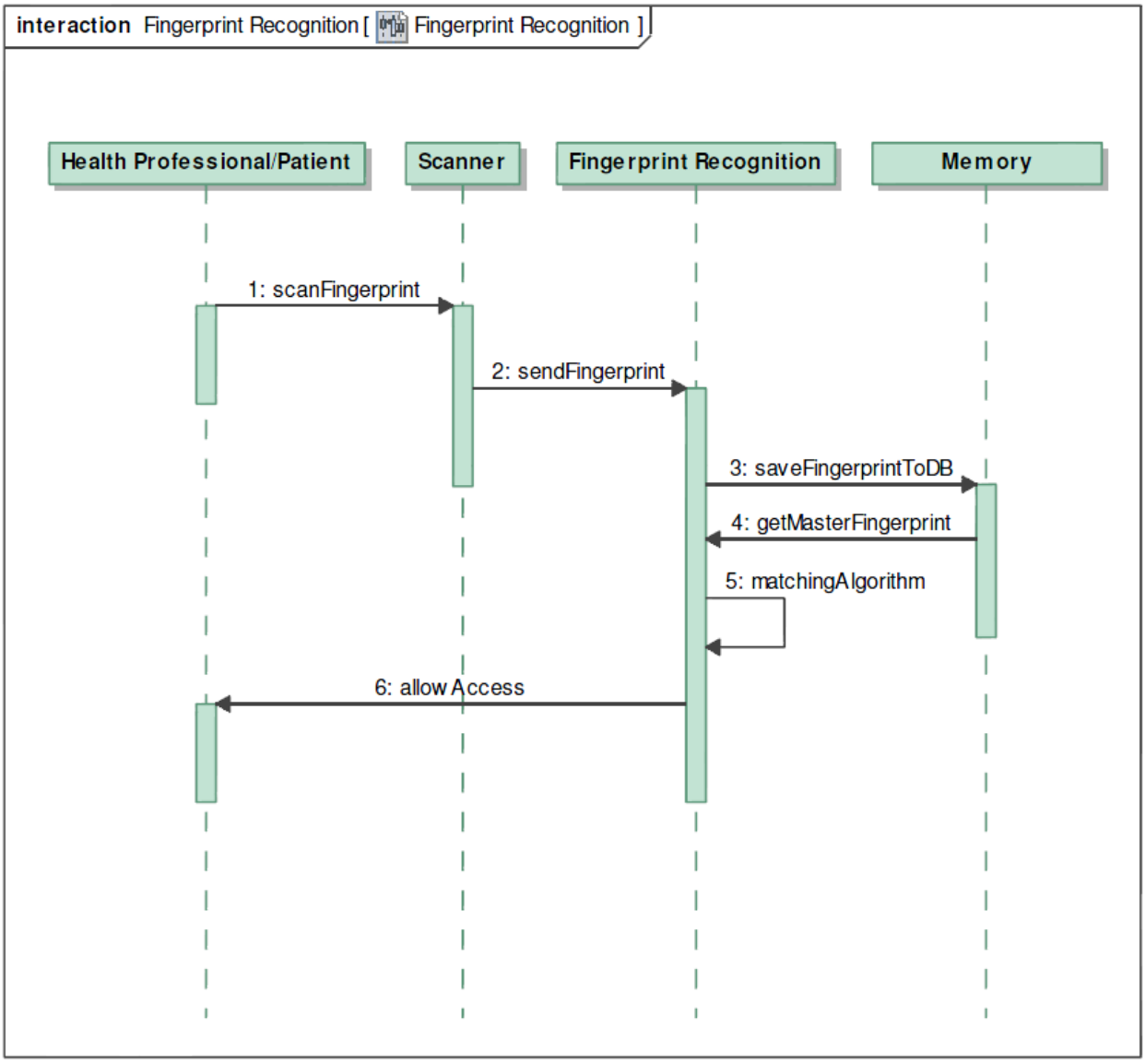


Fingerprint Recognition Behavior

Fingerprint Recognition Activity Diagram

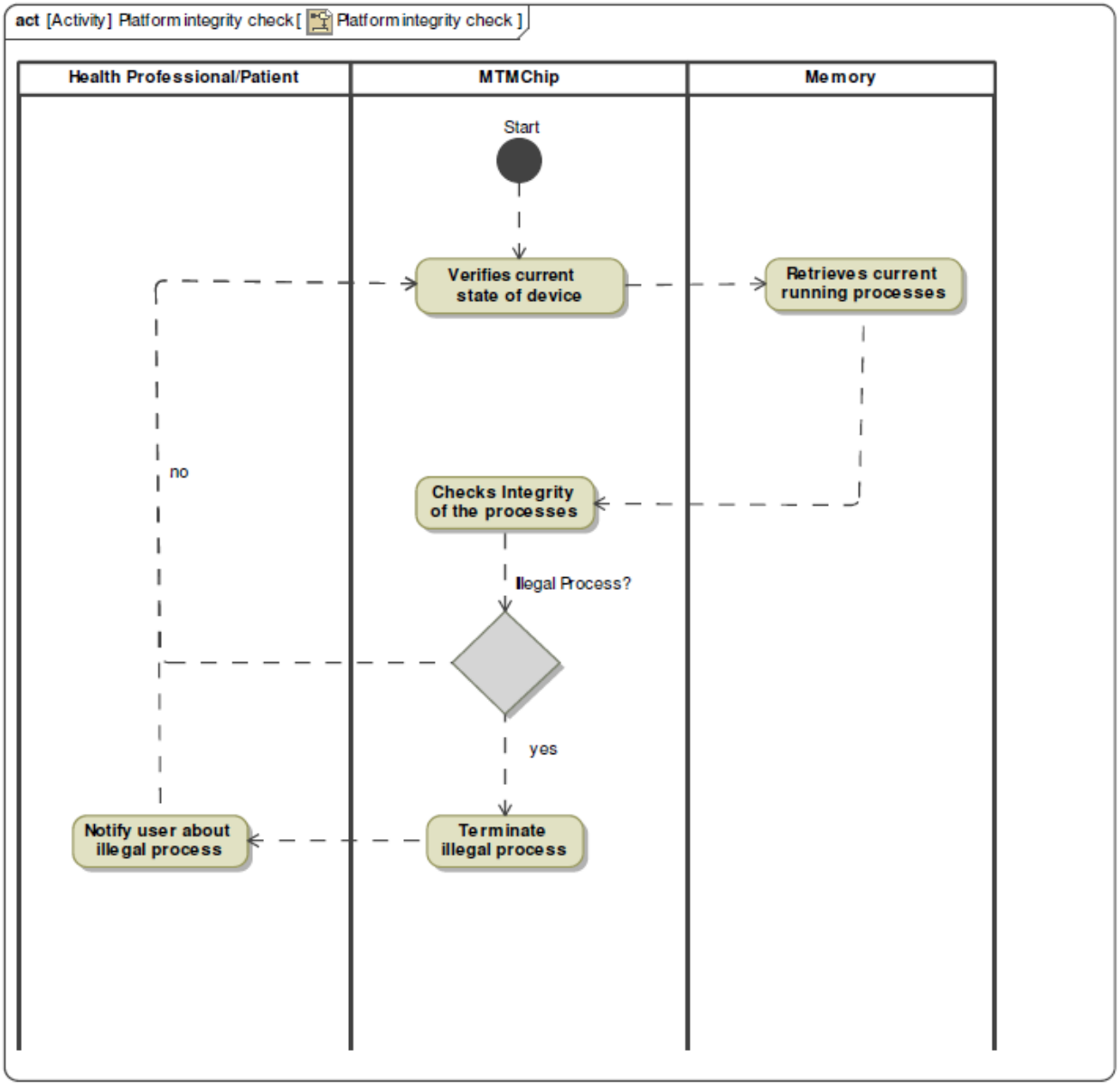


Fingerprint Recognition Sequence Diagram

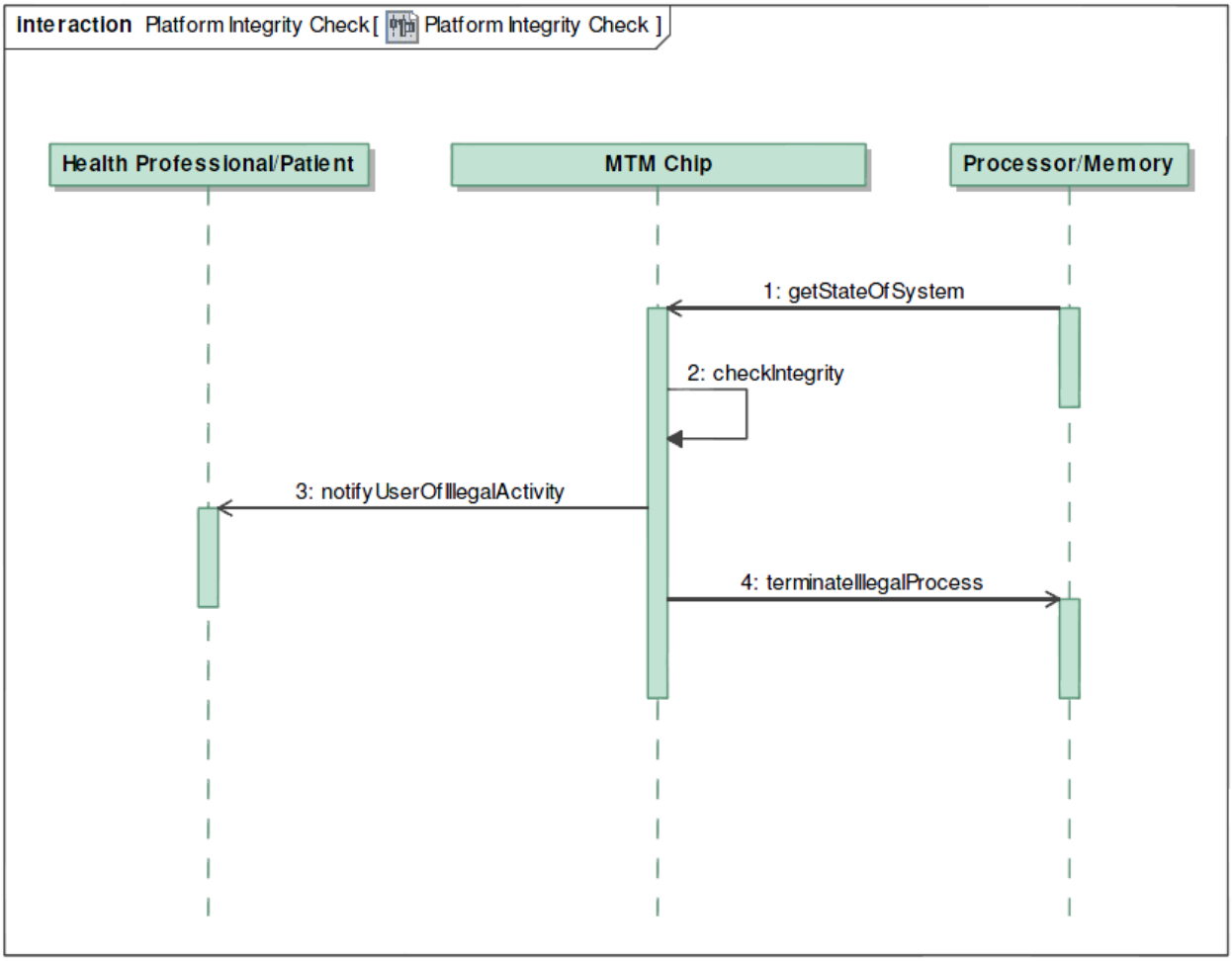


Platform Integrity Check Behavior

Platform Integrity Check Activity Diagram

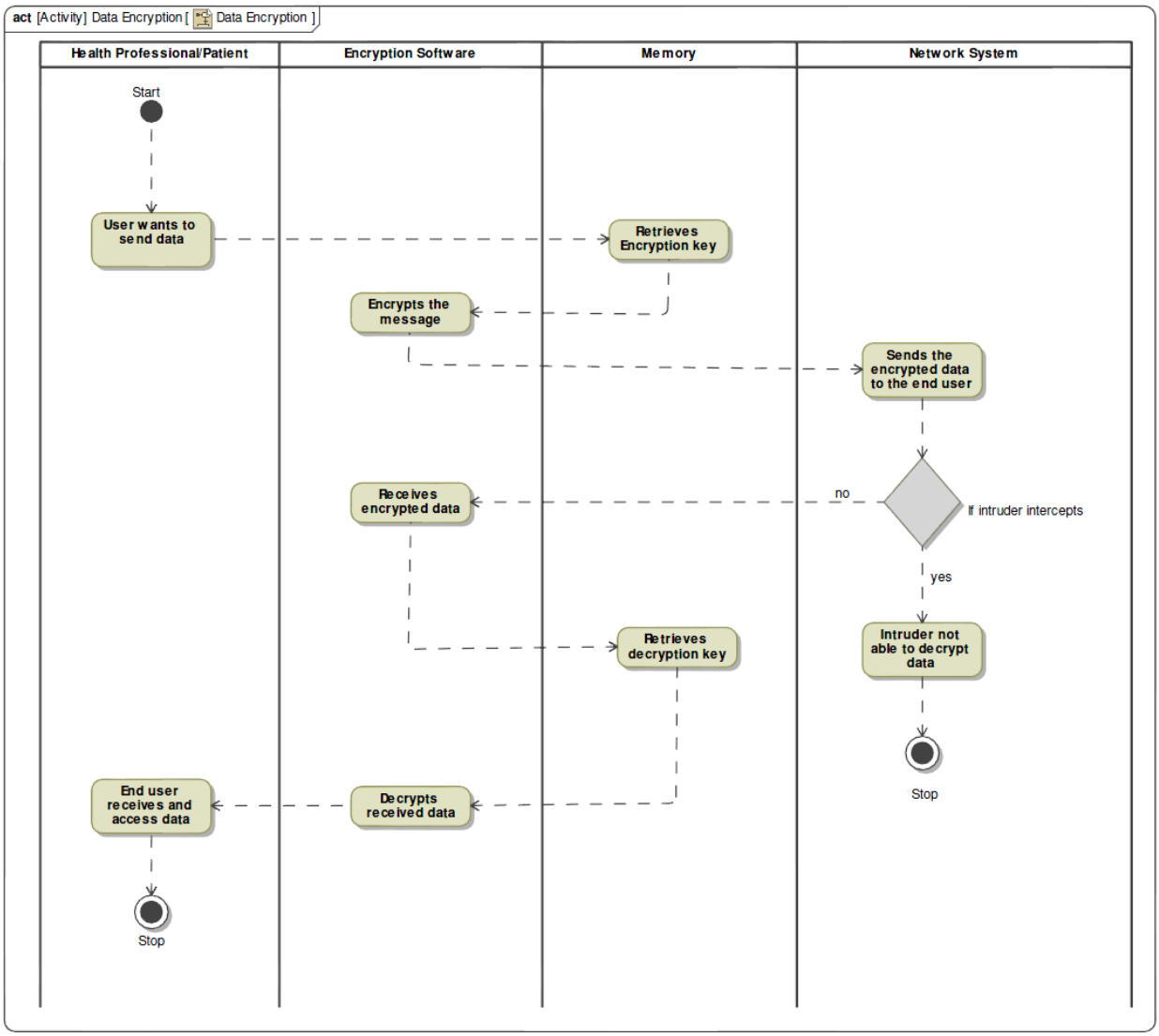


Platform Integrity Check Sequence Diagram

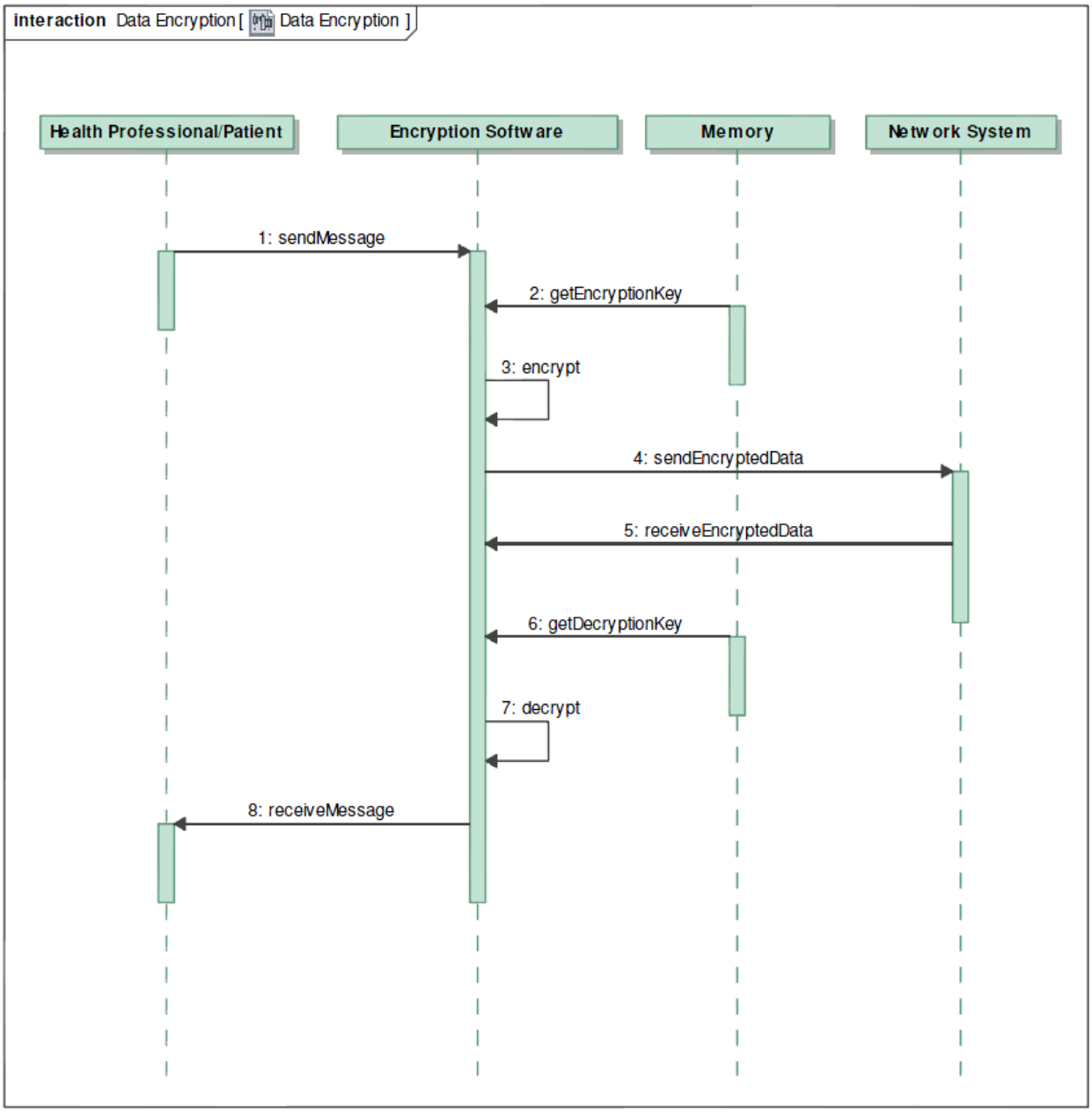


Data Encryption Behavior

Data Encryption Activity Diagram

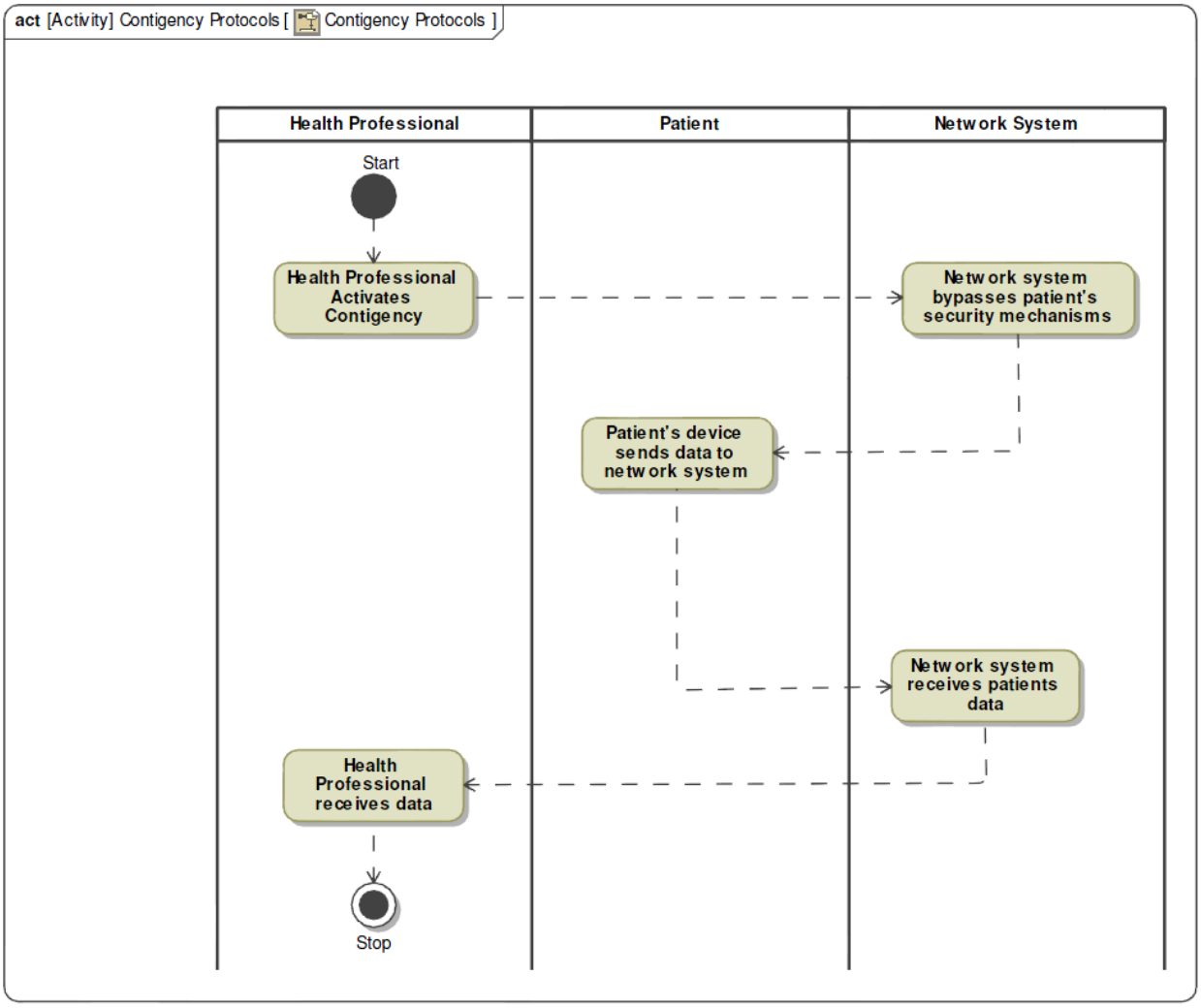


Data Encryption Sequence Diagram

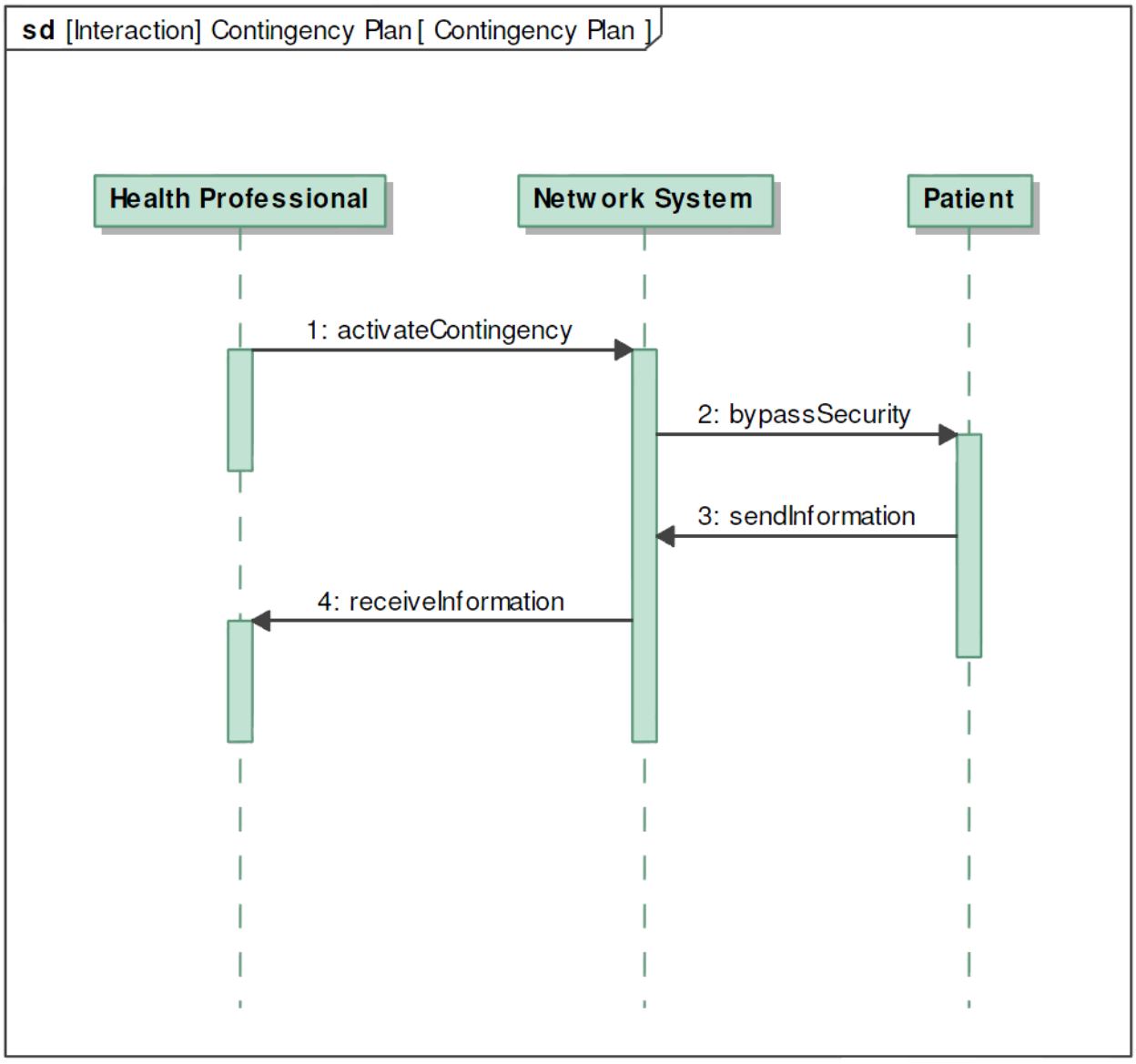


Congtingency Protocols Behavior

Contingency Protocols Activity Diagram



Contingency Protocols Sequence Diagram



Requirements Engineering

Requirements Table

#	Requirements	Description
1	Voice Recognition Requirements	
2	1.a	The microphone must be able to handle sound levels up to 100dB.
3	1.b	The voice recognition algorithm must be able to handle frequency ranges between 300Hz - 3500Hz.
4	1.c	The time it takes to match the voice must not exceed 100 milliseconds.
5	1.d	The voice recognition algorithm must have a success rate of at least 99%.
6	1.e	The voice recognition software must not cost more than $250.
7	Fingerprint Recognition Requirements	
8	2.a	The time it takes to match the fingerprint must not exceed 100 milliseconds.
9	2.b	The time it takes to enroll the fingerprint must not exceed 300 milliseconds.
10	2.c	The fingerprint recognition algorithm must have a success rate of at least 99%.
11	2.d	The maximum memory that can be allocated for the fingerprint recognition software must not exceed 4MB.
12	2.e	The maximum template size for the fingerprint must not exceed 2KB.
13	2.f	The fingerprint scanner and software must not cost more than $75.
14	Data Encryption Requirements	
15	3.a	The encryption algorithm must have a throughput of at least 50MiB/s.
16	3.b	The encryption algorithm is secure to prevent interception of data.
17	3.c	Able to correct small errors in the bit-stream.
18	Platform Integrity Check Requirements	
19	4.a	Checking processes should not be computationally intensive.
20	4.b	MTM chip should be robust and be physically durable to damage (otherwise, failure of chip would lead to loss of data).
21	4.c	MTM software must be compatible with wireless device.
22	4.d	The MTM chip must not cost more than $100.
23	Overall System Requirements	

24	5.a	Cost of systems must fall within wireless device budget.
25	5.b	Weight of systems must fall within wireless device specifications.
26	5.c	Size of systems must be able to fit within wireless device.
27	Additional Components Requirements	
28	6.a	The size of memory should be at least 512 MB and should be clocked at 600 MHz.
29	6.b	Processor speed should be 1GHz single core.
30	6.c	The battery should have a minimum of 1500 mAH and a minimum battery life of 12 hours

Voice Recognition Requirements Diagram

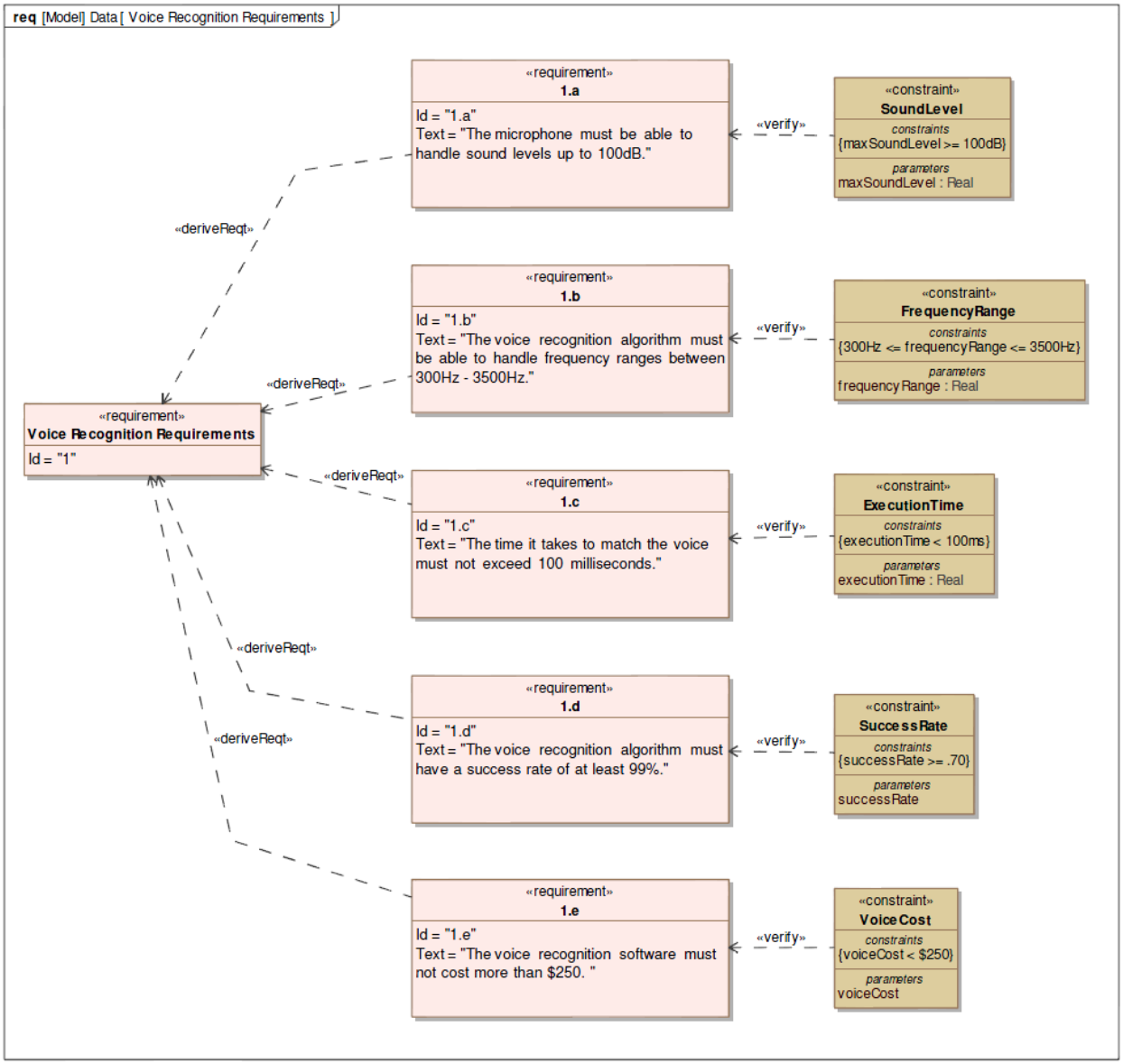
1.a. The microphone must be able to handle sound levels up to 100dB.

1.b. The voice recognition algorithm must be able to handle frequency ranges between 300Hz - 3500Hz.

1.c. The time it takes to match the voice must not exceed 100 milliseconds.

1.d. The voice recognition algorithm must have a success rate of at least 99%.

1.e. The voice recognition software must not cost more than $250.



Fingerprint Recognition Requirements Diagrams

2.a. The time it takes to match the fingerprint must not exceed 100 milliseconds.

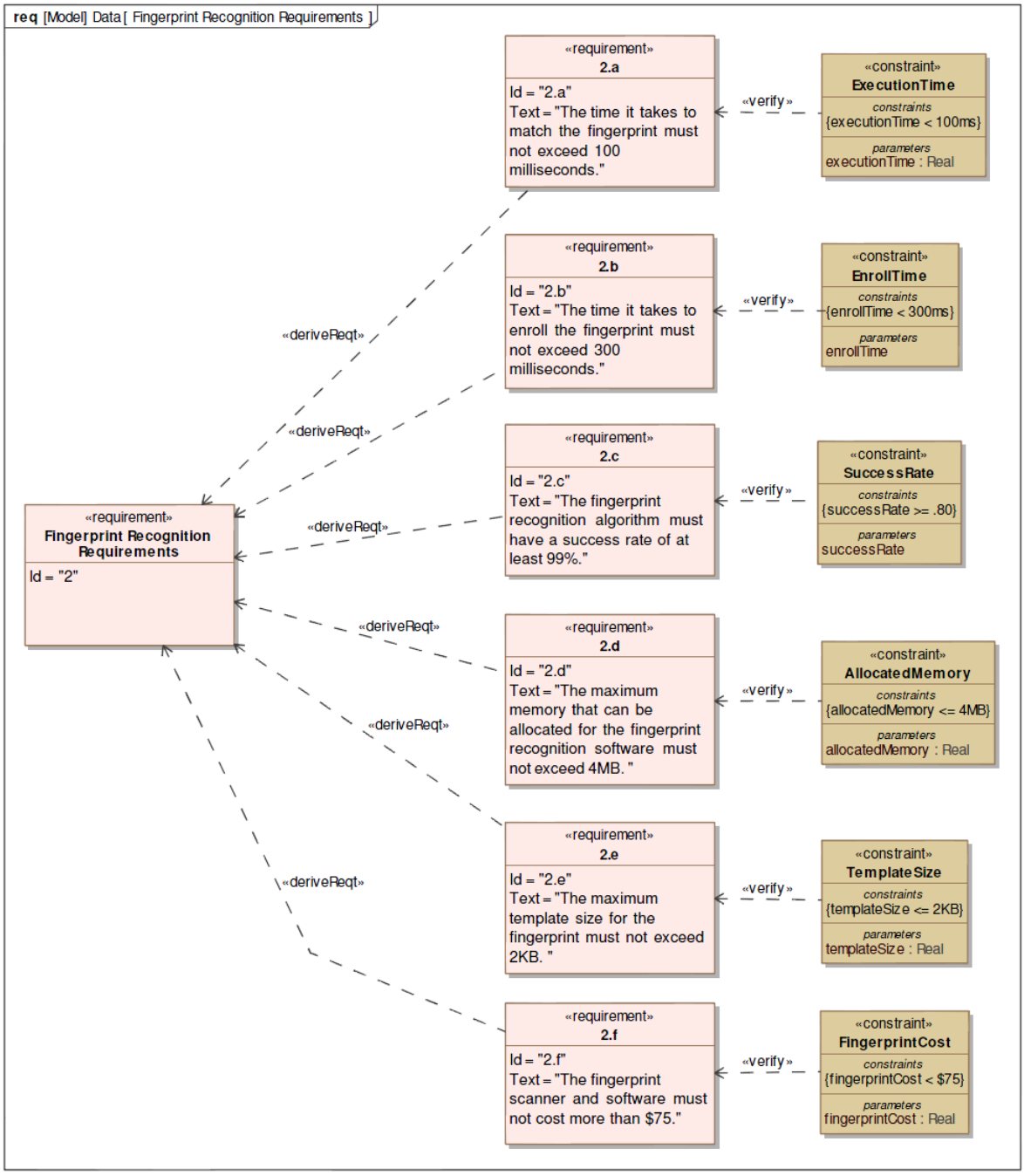
2.b. The time it takes to enroll the fingerprint must not exceed 300 milliseconds.

2.c. The fingerprint recognition algorithm must have a success rate of at least 99%.

2.d. The maximum memory that can be allocated for the fingerprint recognition software must not exceed 4MB.

2.e. The maximum template size for the fingerprint must not exceed 2KB.

2.f. The fingerprint scanner and software must not cost more than $75.

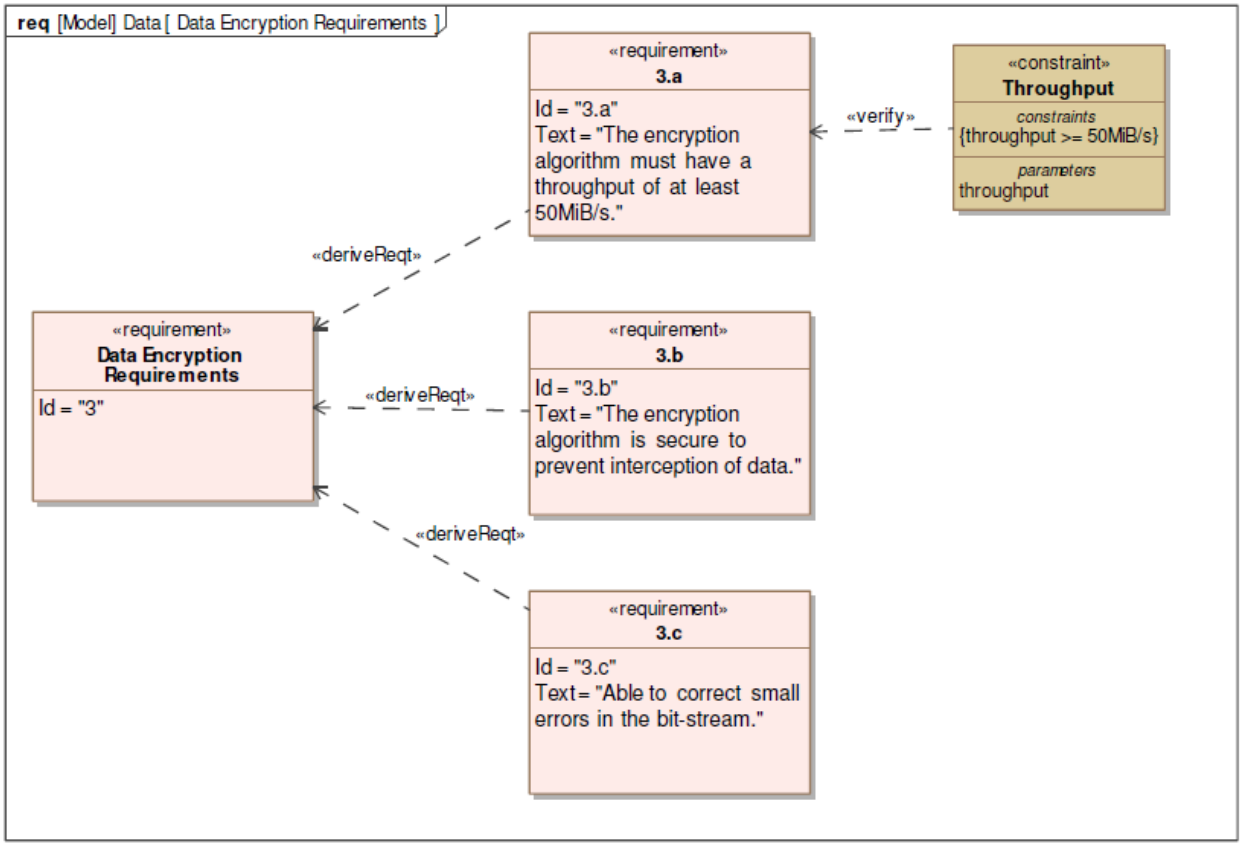


Data Encryption Requirements Diagram

3.a. The encryption algorithm must have a throughput of at least 50MiB/s

3.b. The encryption algorithm is secure to prevent interception of data.

3.c. Able to correct small errors in the bit-stream.



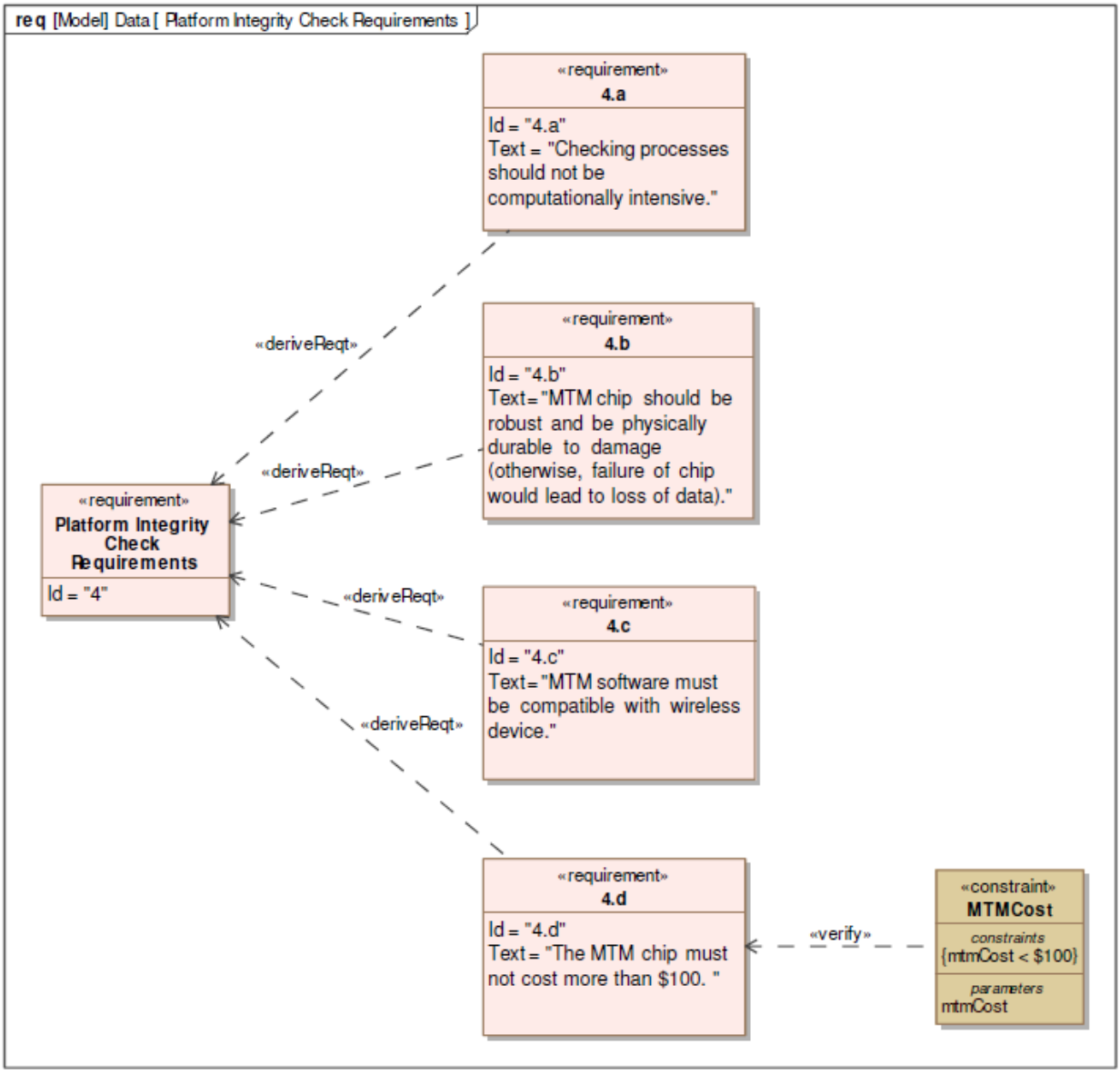
Platform Integrity Check Requirements Diagram

4.a. Checking processes should not be computationally intensive.

4.b. MTM chip should be robust and be physically durable to damage (otherwise, failure of chip would lead to loss of data).

4.c. MTM software must be compatible with wireless device.

4.d. The MTM chip must not cost more than $100.

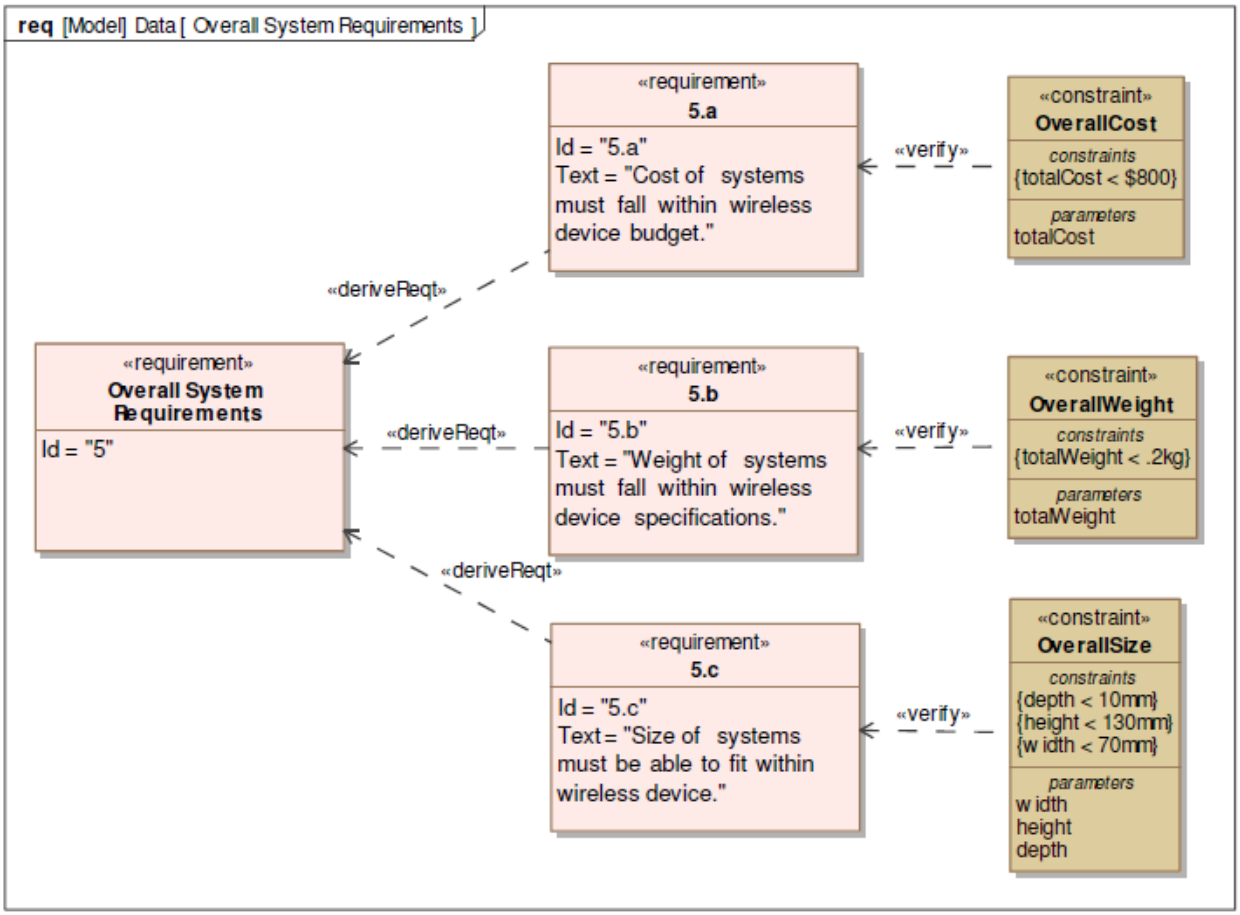


Overall System Requirements Diagram

5.a. Cost of systems must fall within wireless device budget.

5.b. Weight of systems must fall within wireless device specifications.

5.c. Size of systems must be able to fit within wireless device.

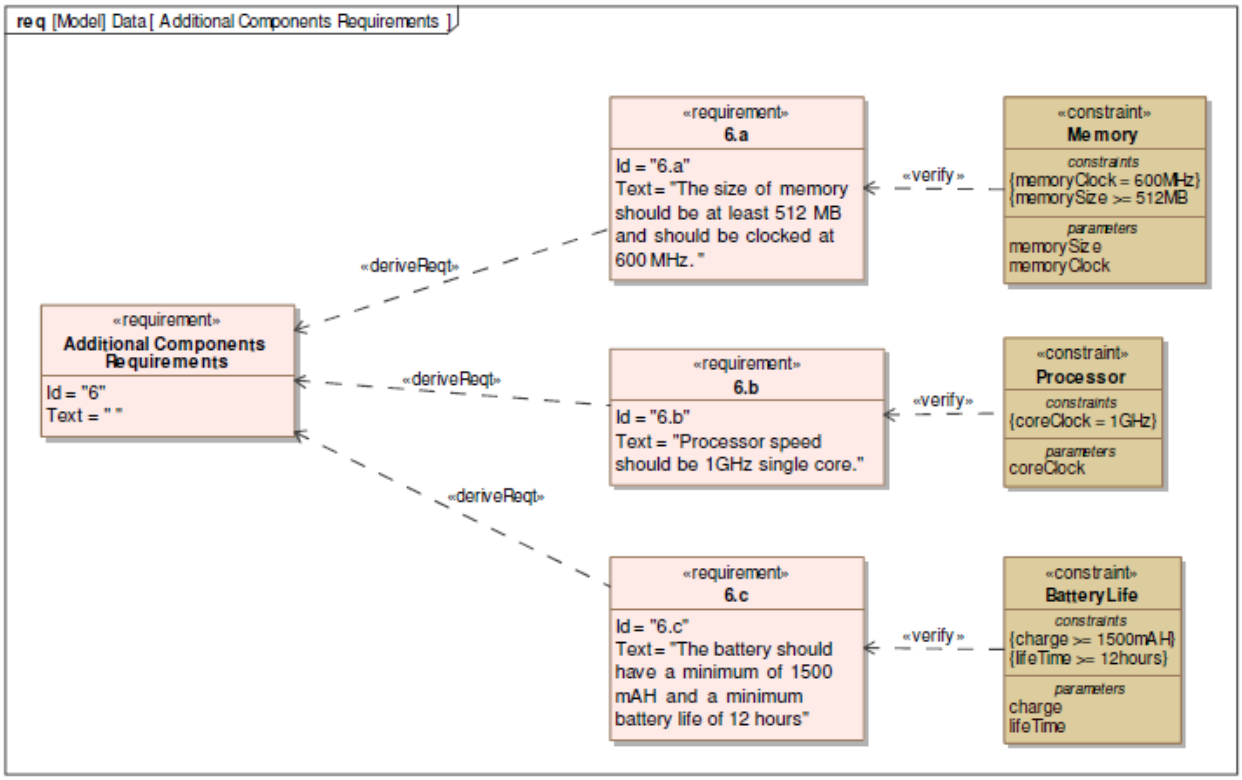


Additional Components Requirements

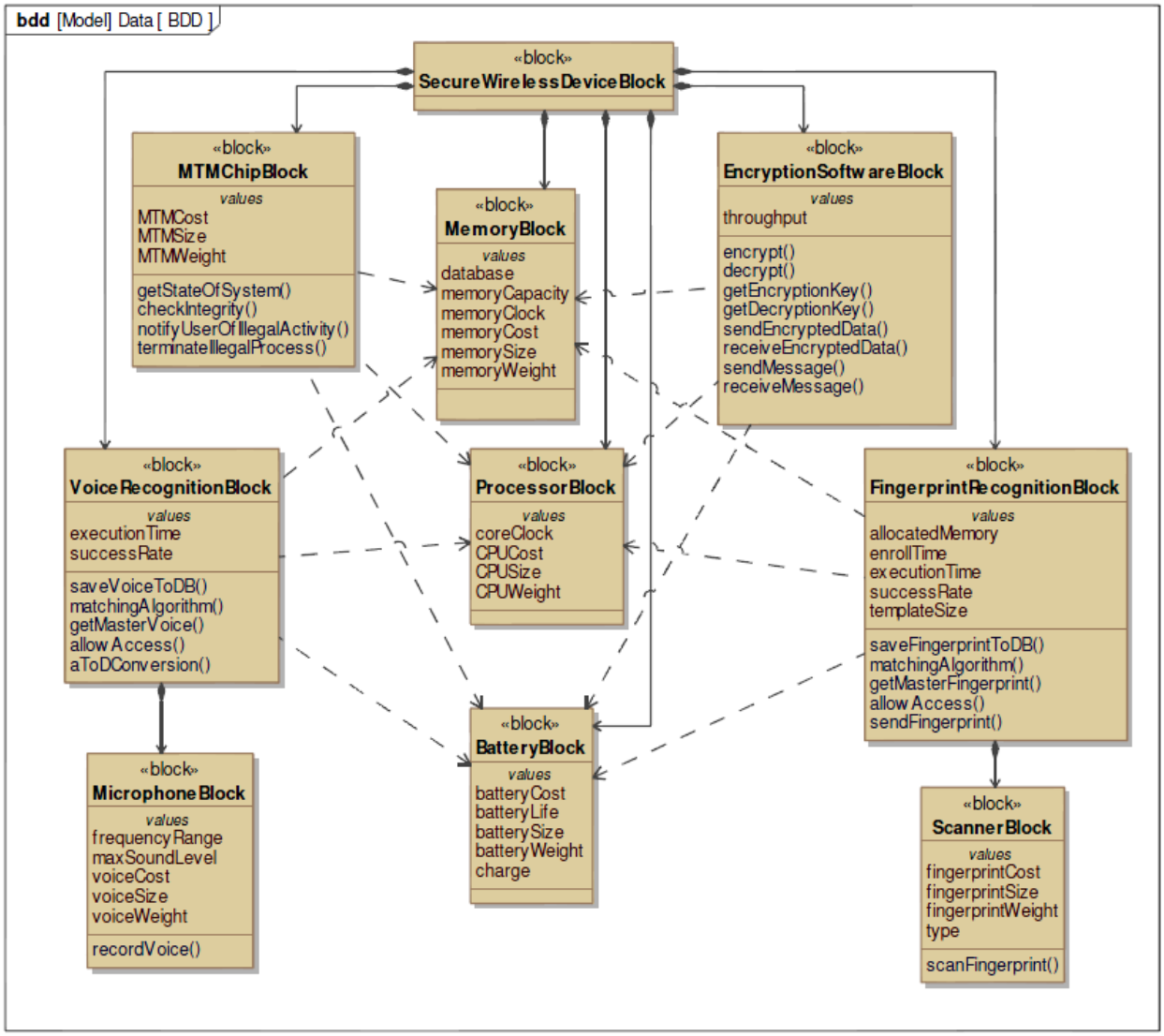
6.a. The size of memory should be at least 512 MB and should be clocked at 600 MHz.

6.b. Processor speed should be 1 GHz single core.

6.c. The battery should have a minimum of 1500 mAH and a minimum battery life of 12 hours.

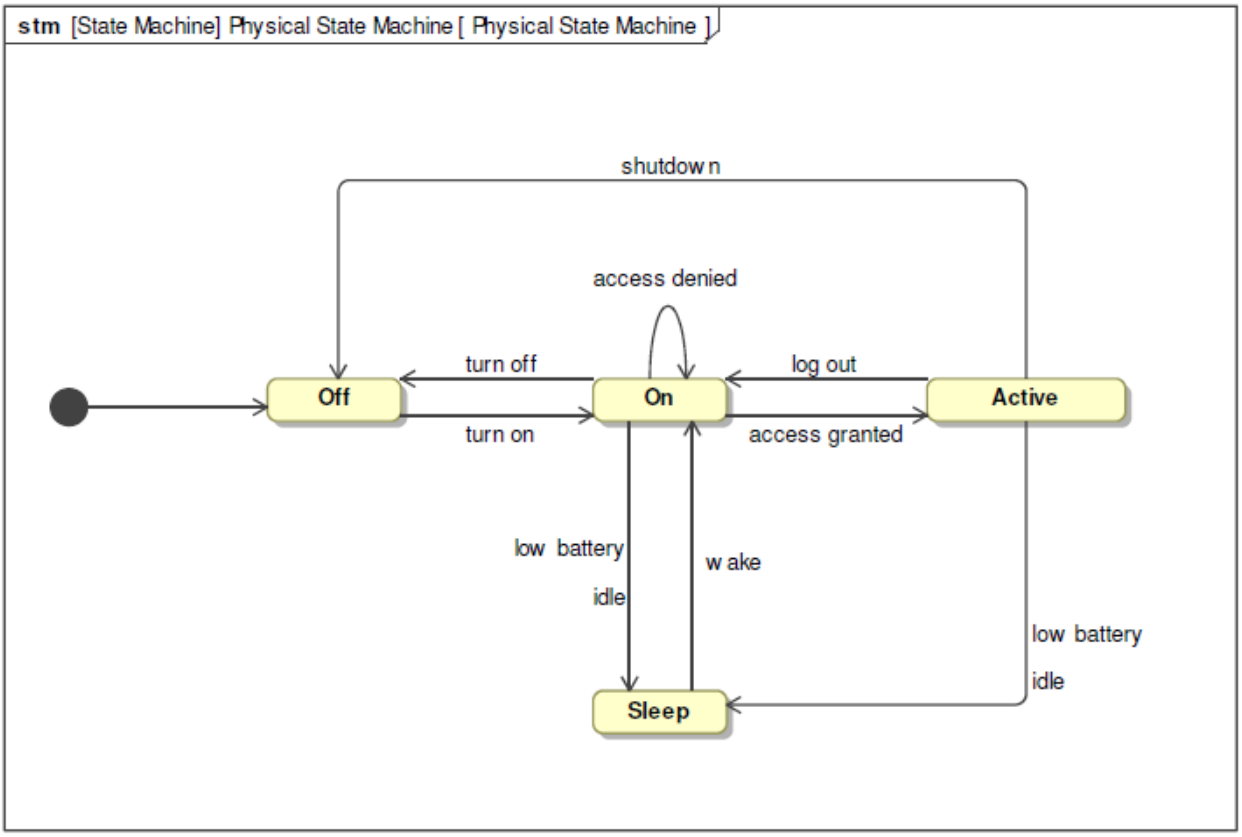


System-Level Design

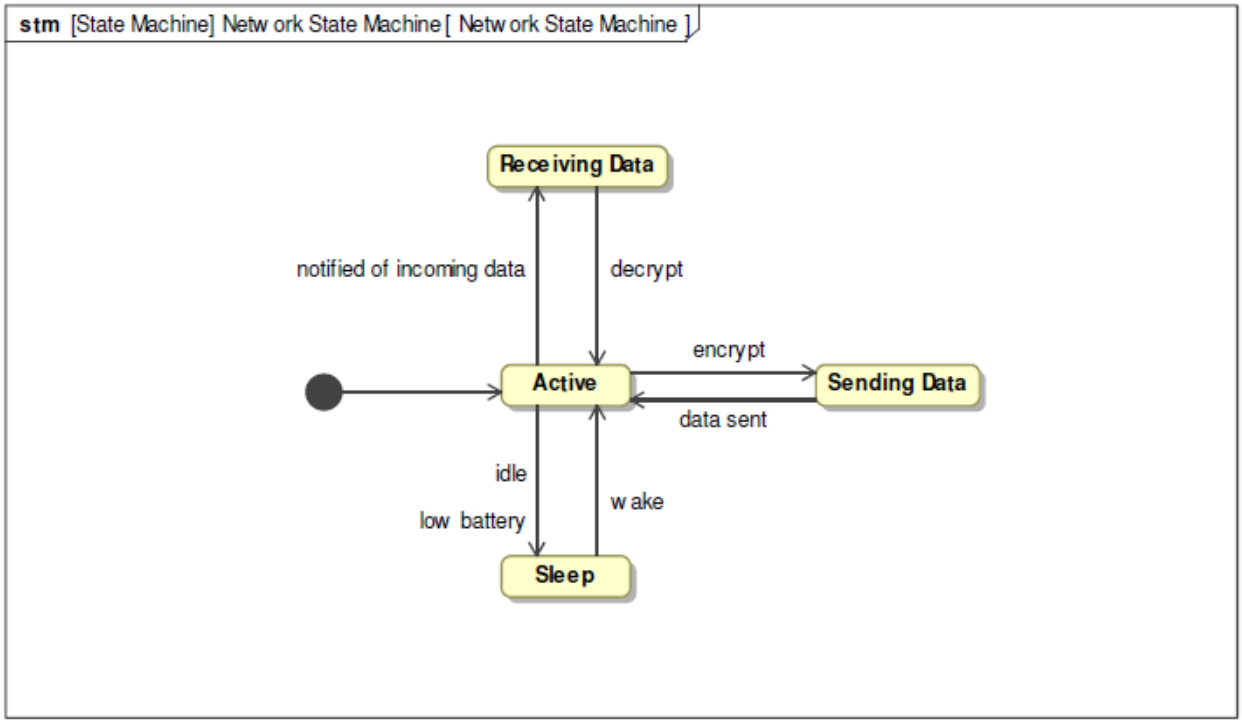


State Diagrams

Physical State Machine

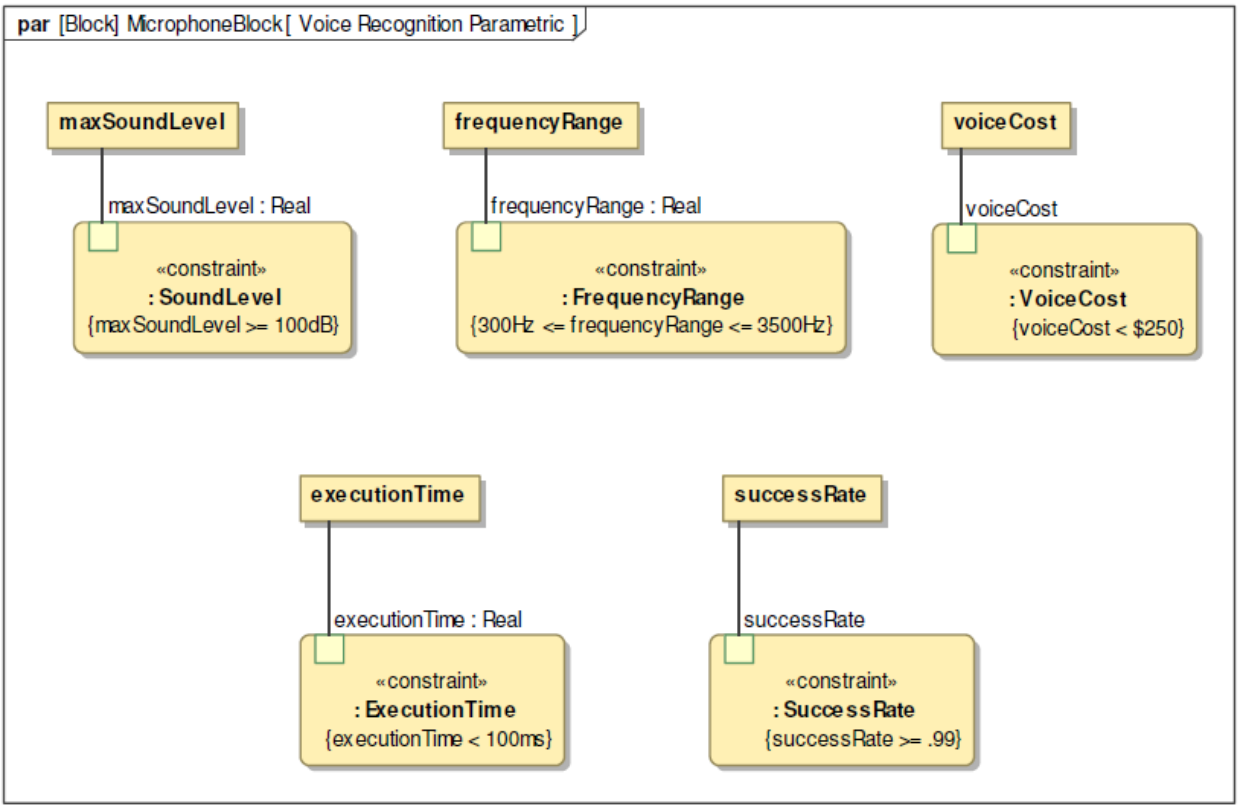


Network State Machine

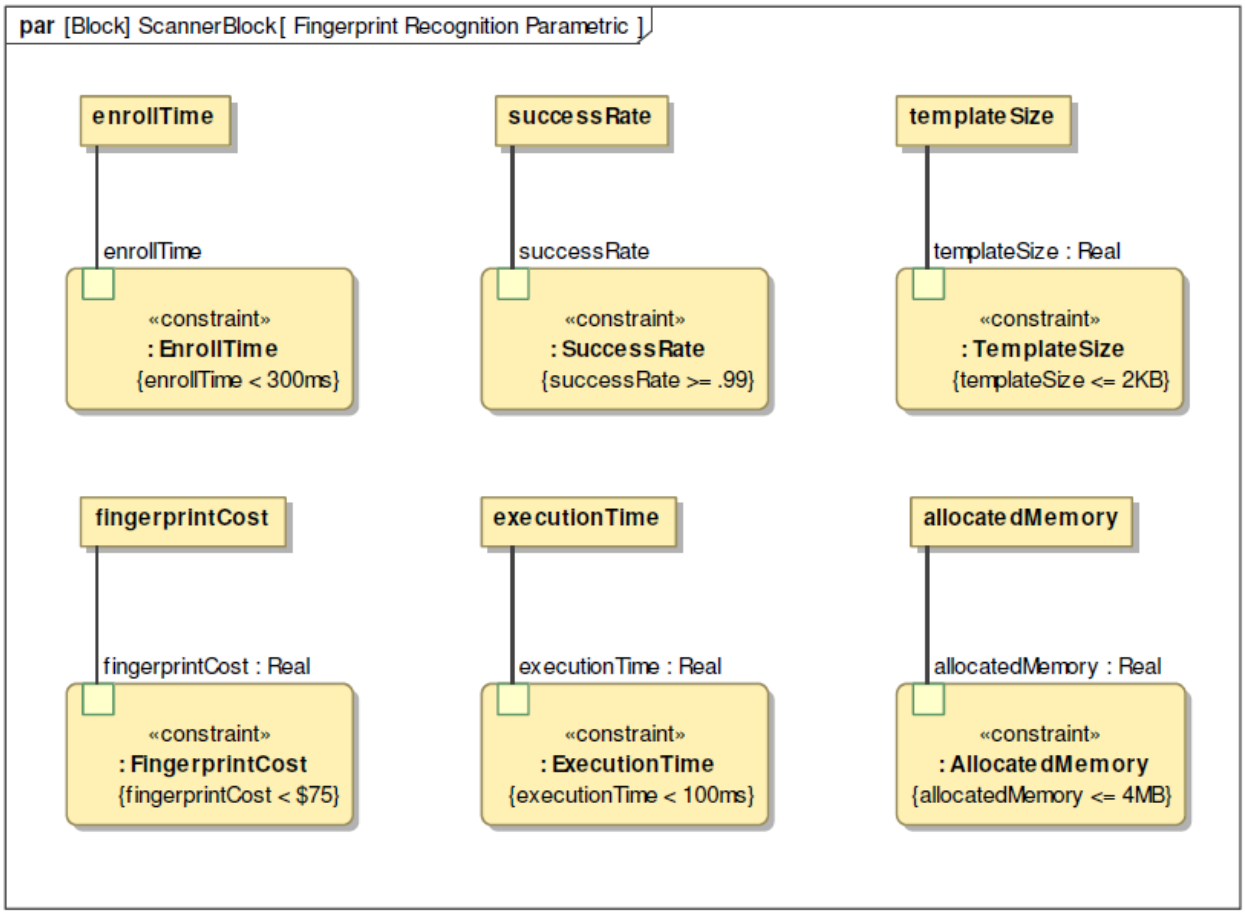


Parametric Diagrams

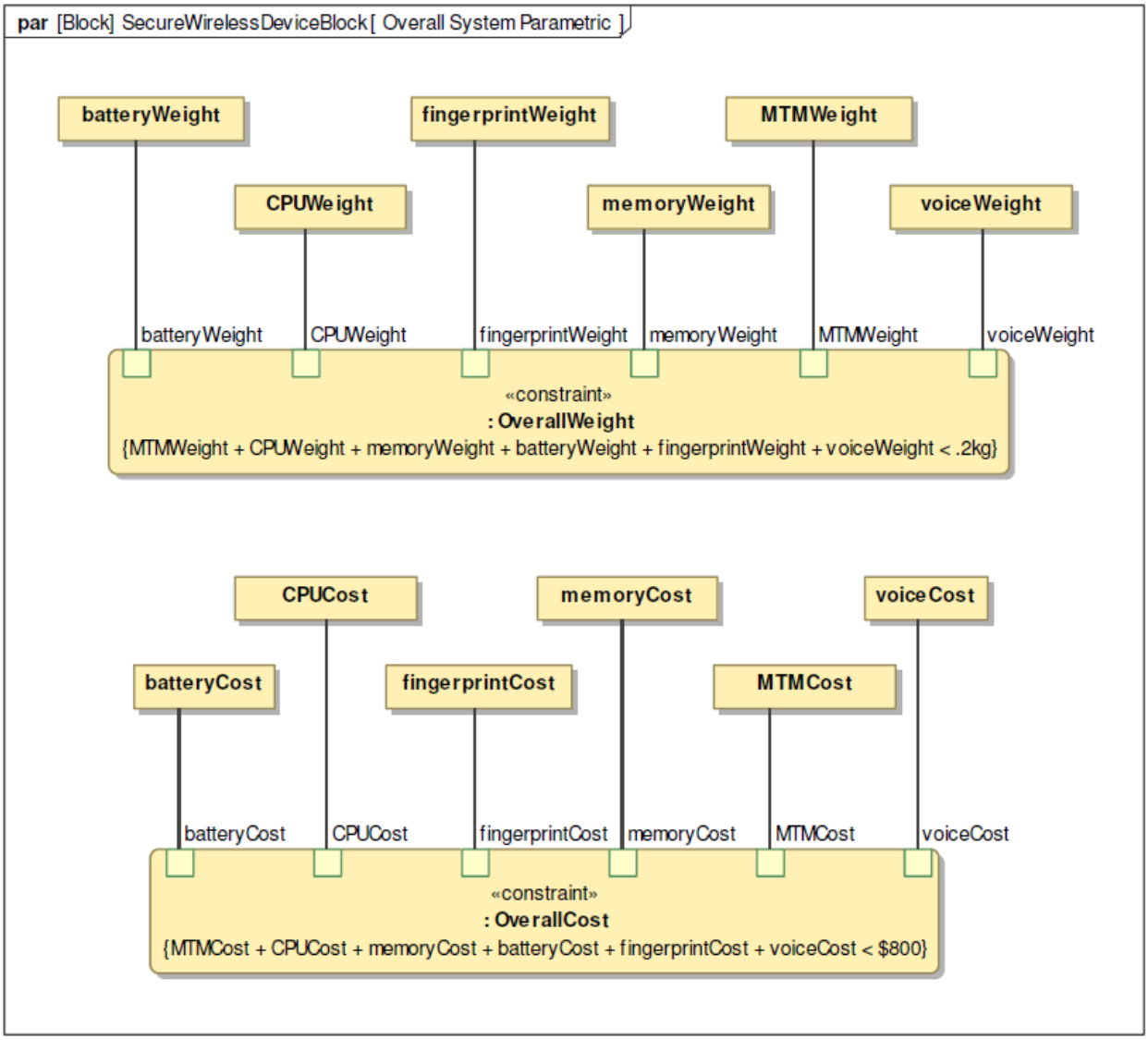
Voice Recognition Parametric Diagrams



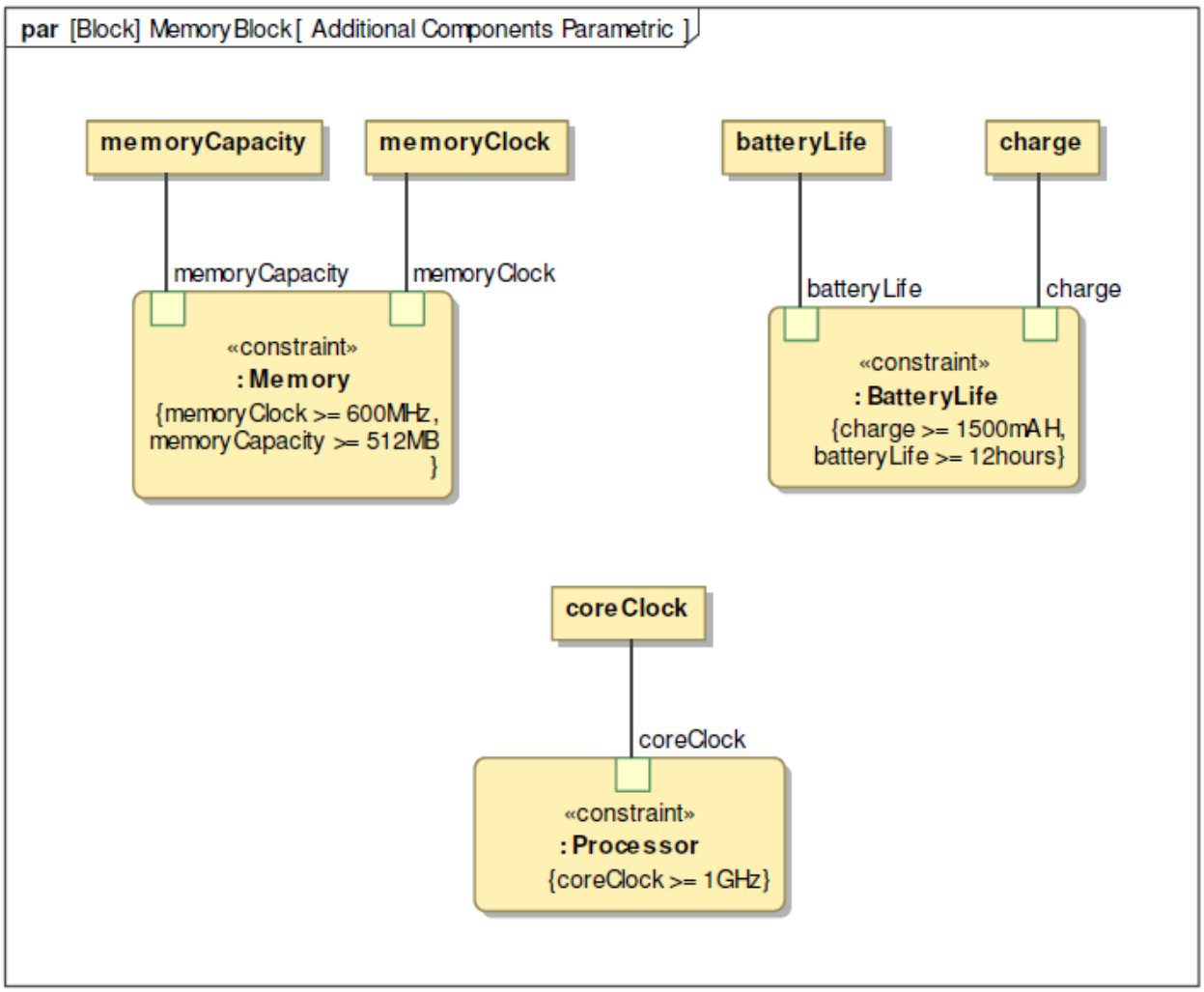
Fingerprint Recognition Parametric Diagrams



Overall System Parametric Diagrams



Additional System Parametric Diagrams



Simplified Approach to Trade-Off Analysis

A trade-off analysis can be performed on the fingerprint hardware, fingerprint algorithm, voice recognition software, and communication encryption. Voice recognition requires no hardware assuming there is an adequate microphone for the mobile device.

We researched at least three different options for each component. The system components metrics are Cost, TimeCost and Security level. Cost is the per-unit price, including licensing of software. TimeCost is the average time it takes for the specified component to complete a task, measured in milliseconds. For example, the TimeCost of the fingerprint algorithm depends on the matching time. The security level depends on the specific component, for example to measure security in fingerprint algorithms we chose the Equal Error Rate, since it best describes the overall error rate of an algorithm. An algorithm with the lowest EER has the highest security level. The security level is a normalized value, bounded between 0 and 1, with 1 being the most secure option out of all.

Data Table 1

Component	Cost ($)	TimeCost(ms)	Security level(0-1)	Referenced
FingerPrintHardware				
FingerPrintHardware1	15	-	0.65	Lenovo Fingerprint Reader Card
FPH2	33	-	0.67	Eikon To Go Digital Privacy Manager
FPH3	64	-	1	Hopkami USB Fingerprint Sensor/ Fingerprint Scanner
FingerPrintAlgorithm				
FPA1	-	46	1	P129
FPA2	-	55	0.96	P133
FPA3	-	48	0.93	P045
VoiceRecognitionSoftware				
VRS1	50	50	0.7	Blackhole Security
VRS2	600	30	1	Dragon Professional
VRS3	120	40	0.6	Dragon Nuance

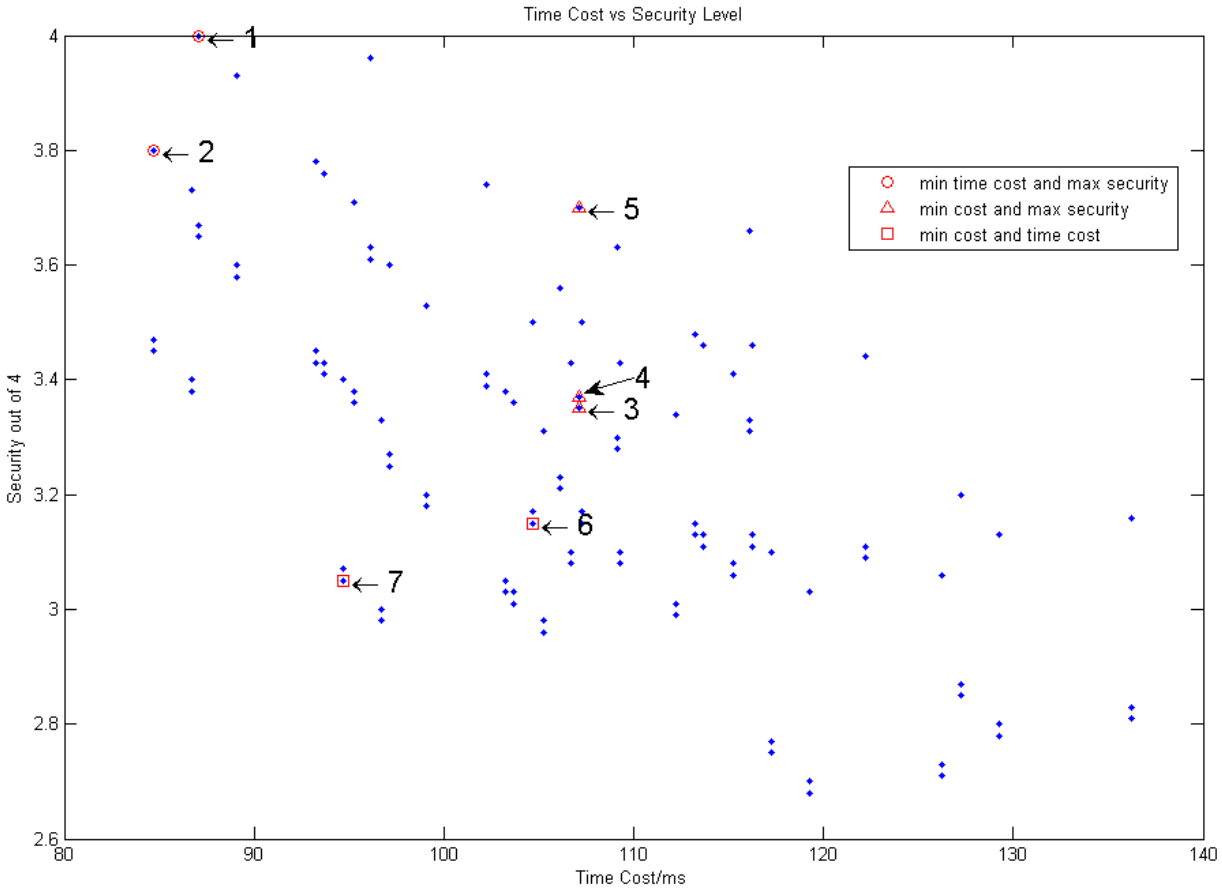
Data Table 2

CommunicationEncryption	Encrption Speed 1Mib/s	Relative Speed	Security Level(0-1)	Specific Encryption
AES -128bit	115	1	0.8	AES/CBC (128-bit key), AES/CTR (128-bit key)
AES-256bit	90	0.78	1	AES/CTR (256-bit key), AES/CBC (256-bit key)
Blowfish	58	0.5	0.78	Blowfish/CTR
DES-56bit	32	0.28	0.5	DES/CTR

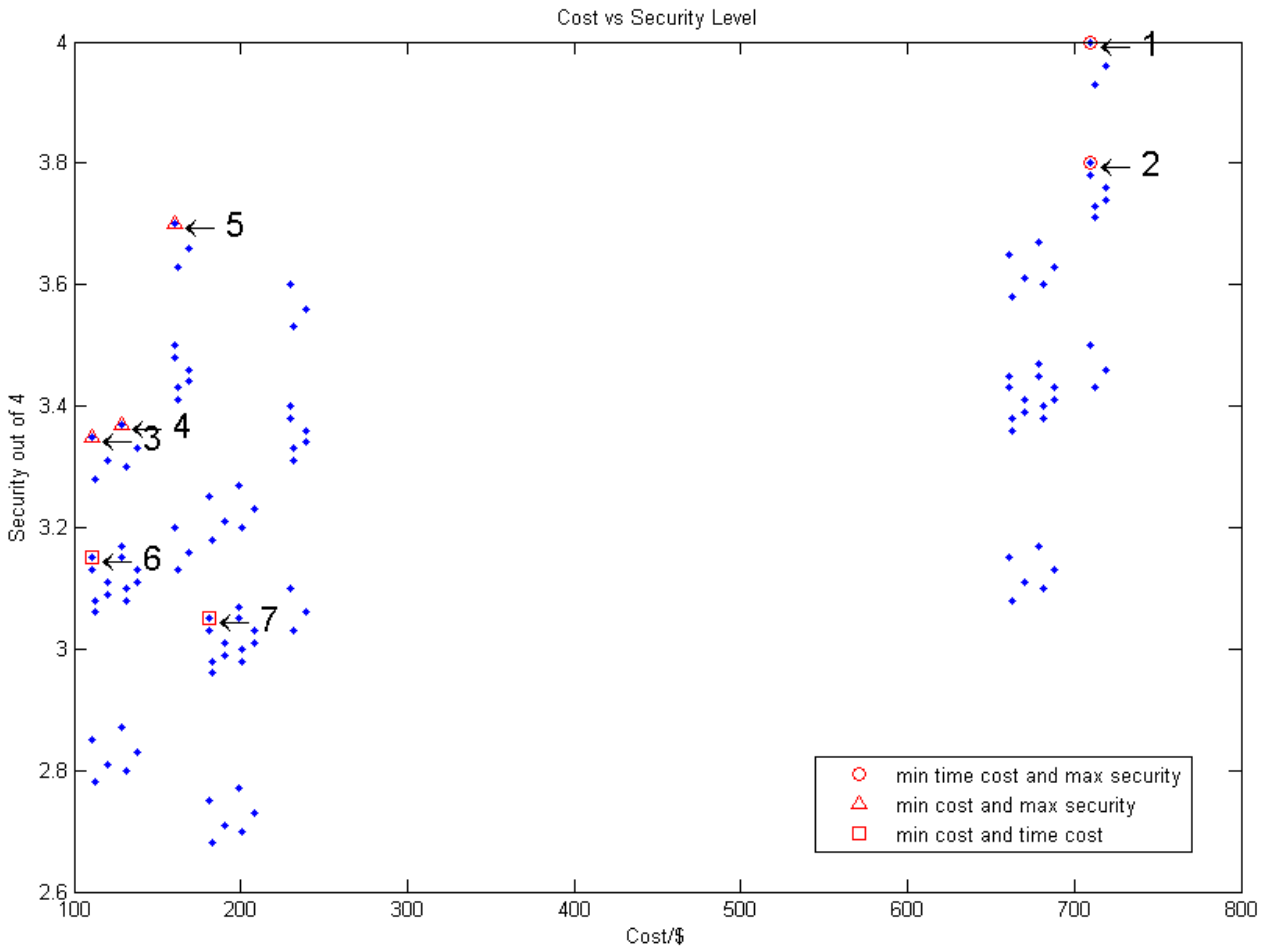
Analysis Plots

Point #	FingerPrintHardware	FingerPrintAlgorithm	VoiceRecognition	Encryption
1	FPH3 (Full scan)	FPA1 (P129)	VRS2 (Drag Pro)	AES-256bit
2	FPH3 (Full Scan)	FPA1 (P129)	VRS2 (Drag Pro)	AES-128bit
3	FPH1 (Slit Scan)	FPA1 (P129)	VRS1 (BlackHole)	AES-256bit
4	FPH2 (+USB interface)	FPA1 (P129)	VRS1 (BlackHole)	AES-256bit
5	FPH3 (Full Scan)	FPA1 (P129)	VRS1 (BlackHole)	AES-256bit
6	FPH1 (Slit Scan)	FPA1 (P129)	VRS1 (BlackHole)	AES-128bit
7	FPH1 (Slit Scan)	FPA1 (P129)	VRS3 (Dragon)	AES-128bit

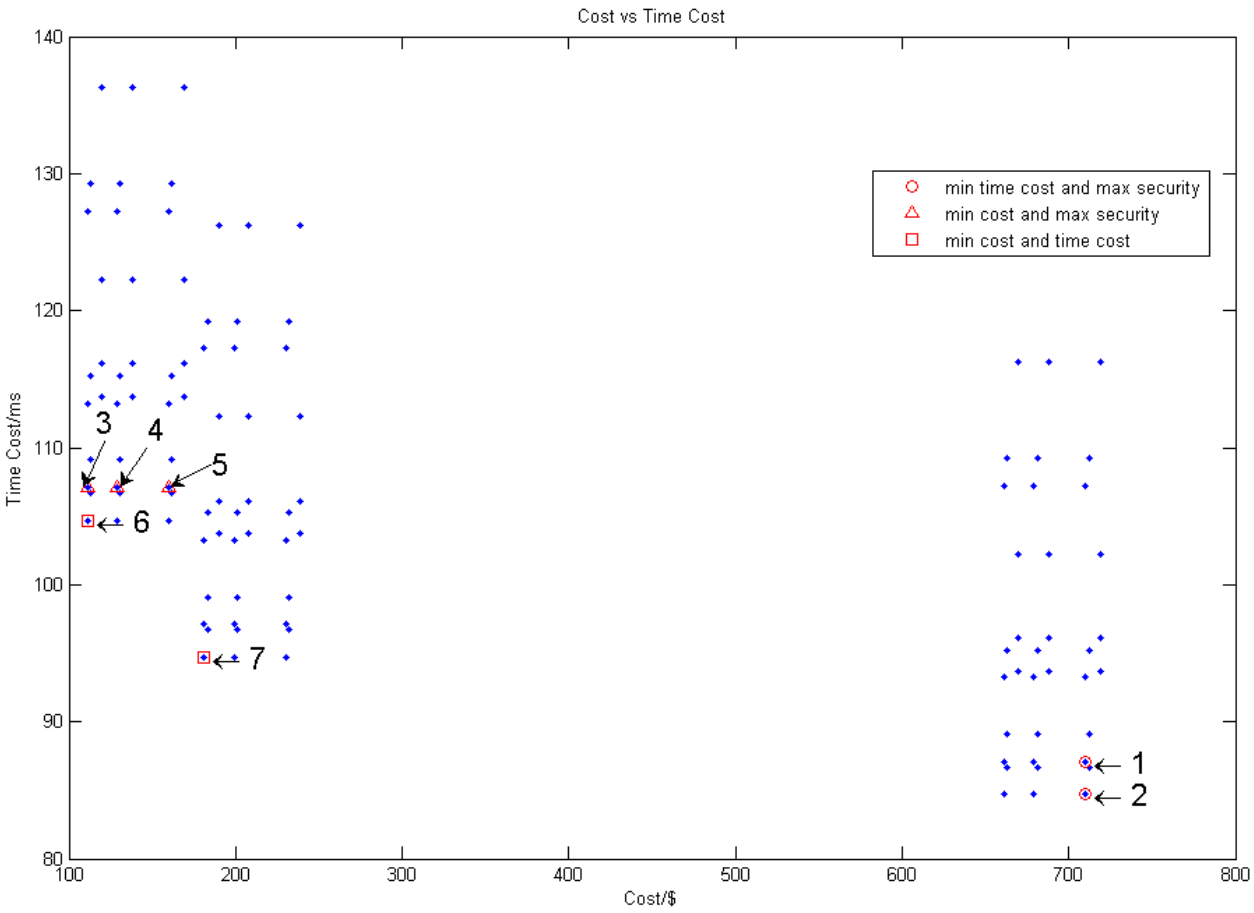
This table shows the chosen fingerprint hardware, fingerprint algorithm, voice recognition, and encryption combination for the points in the following plots.



The time delay of one trial of login and 1 minute communication is plotted versus security level for different combinations of the device. Point 1 and point 2 gives the best solution for maximizing security level and minimizing time cost. The other points maximize other criterion, and are shown for comparison purpose.



Components cost for overall device and security level is plotted for all choice of components. Points 3, 4, and 5 dominant the other points, and is the prime solution cost wise. The time cost solution (points 1, 2) has much higher cost.



The time delay of one trial of login and 1 minute communication is plotted versus components cost for the overall device. Points 6 and 7 are the best solutions for minimizing time cost and component cost.

Summary and Conclusions

The device we have proposed provides a solution to the current privacy and convenience issues in the health care system. The device will be user friendly to both patients and health professionals. At the same time, it will be able to provide high level security to prevent unauthorized users to access important data. The device will be similar to a smart phone in terms of weight and size but would be supreme in terms of performance and security. The device can also be customized depending on a hospital's or health care system's requirement but all devices will include the essential security package which is fingerprint recognition, voice recognition, Mobile Trusted Module Chip and encryption software.

The device can also be extended to military communications and smart grid communications. Since, secure devices are of utmost importance in military communications, the Department of Defense could also make use of the device.

Based on our evaluations of cost, security and performance the points we chose to be the best combination of options are:

Performance vs. Security	1, 2
Security vs. Cost	3, 4, 5
Cost vs. Performance	6, 7
Overall System	3, 4, 5

The set of above points is all feasible and can be tailored towards a particular customer's demands and requirements. In general, the set of points (3, 4, and 5) is recommended. The performance variation between the different security mechanisms is negligible to human perception.

The trade off analysis suggests that for higher security the cost for the device will be higher. Depending on the requirements of the customer, the device can be specified to be highly secure with a high cost or reasonable security with a medium cost. From our trade off analysis we have determined that the combinations of fingerprint recognition and voice recognition provide the highest security. Removing fingerprint recognition and using just voice recognition or vice versa lowers the security of the device but does not really lower the cost of the device.

The successful combination of the different security mechanisms has been identified to provide the best cost, security, and performance for wireless device security. The best ratio of these metrics will benefit stakeholders by simplifying the complexity of searching for security mechanisms for their wireless devices.

References

Baras, J. S., & Radosavac, S. (2005). A Framework for MAC Protocol Misbehavior Detection in Wireless Networks. Retrieved from http://www.ece.umd.edu/~baras/publications/papers/2005/RadosavacBK_2005.pdf

Baras, J. S., Ivanov, V. I., & Yu, P. L. (2009). Securing the Communication of Medical Information Using Local Biometric Authentication and Commercial Wireless Links. Retrieved from http://www.ece.umd.edu/~baras/publications/journals/Ivanov_Yu_Baras_Securing_communication_of_medical_information.pdf

Bennamoun, M., Bhagavatula, V., Hu, J., & Toh, K. (2011, February). Biometric security for mobile computing. Retrieved from http://goanna.cs.rmit.edu.au/~jiankun/SCN-SI-012.pdf

Boncella, J. R. (2002). WIRELESS SECURITY: AN OVERVIEW. Communications of the Association for Information Systems (Volume 9) 269-282. Retrieved from http://www.washburn.edu/faculty/boncella/WIRELESS-SECURITY.pdf

Ekberg, J., & Kylanpaa, M. (2007, November). Mobile Trusted Module (MTM) - an introduction Retrieved from http://research.nokia.com/files/tr/NRC-TR-2007-015.pdf

Elmufti, K., Rajarajan, M., Rakocevic, V., & Weerasinghe, D. (2008, July). Patient's privacy protection with anonymous access to medical services. Retrieved from http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4571049

Fische, S., Stewart, T. E., Mehta, S., Wax, R., & Lapinsky, S. E. (2002, October). Handheld Computing in Medicine. Retrieved from http://www.ncbi.nlm.nih.gov/pmc/articles/PMC150367/

Gutierrez, C. N., Kakani, G., Verma, R. C., & Wang, T. (2010, June) .Digital Watermarking of Medical Images for Mobile Devices. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5504666

Hay, R. (2003, November). Physical Security: A Biometric Approach. Retrieved from http://www.sans.org/reading_room/whitepapers/physcial/physical-security-biometric-approach_1325

IBM Corporation Software Group. (2010, February). IBM solutions for cybersecurity: Solutions for mitigating threats in the government sector. Retrieved from ftp://public.dhe.ibm.com/common/ssi/ecm/en/tiw14047usen/TIW14047USEN_HR.PDF

Ju, H., Kim, M., Kim, Y., Park, J., & Park, Y. (2010, February). Design and Implementation of Mobile Trusted Module for Trusted Mobile Computing. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5439136

Jun, S., Kang, D., & Lee, I. (2009) A Study on Migration Scheme for a Mobile Trusted Module. Retrieved from http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=04809395

Maxi-Pedia. (n.d.). Wireless Wi-Fi network security tutorial 101. Retrieved from http://www.maxi-pedia.com/wireless+wifi+network+security+tutorial+101

Pocovnicu, A. (2009). Biometric Security for Cell Phones. Retrieved from http://revistaie.ase.ro/content/49/006%20-%20Pocovnicu.pdf

Schmidt, A. U., Kuntze N., & Kasper M. (2007, December). On the deployment of Mobile Trusted Modules. Retrieved from http://arxiv.org/PS_cache/arxiv/pdf/0712/0712.2113v1.pdf

Shinder, D. (2005, April). Securing Your Pocket PC. Retrieved from http://www.windowsecurity.com/articles/Securing-Pocket-PC.html