

**Politechnika
Warszawska**

**Bezpieczny węzeł czujnikowy
oparty na IoT**

Praca dyplomowa magisterska

Maciej Krysiak



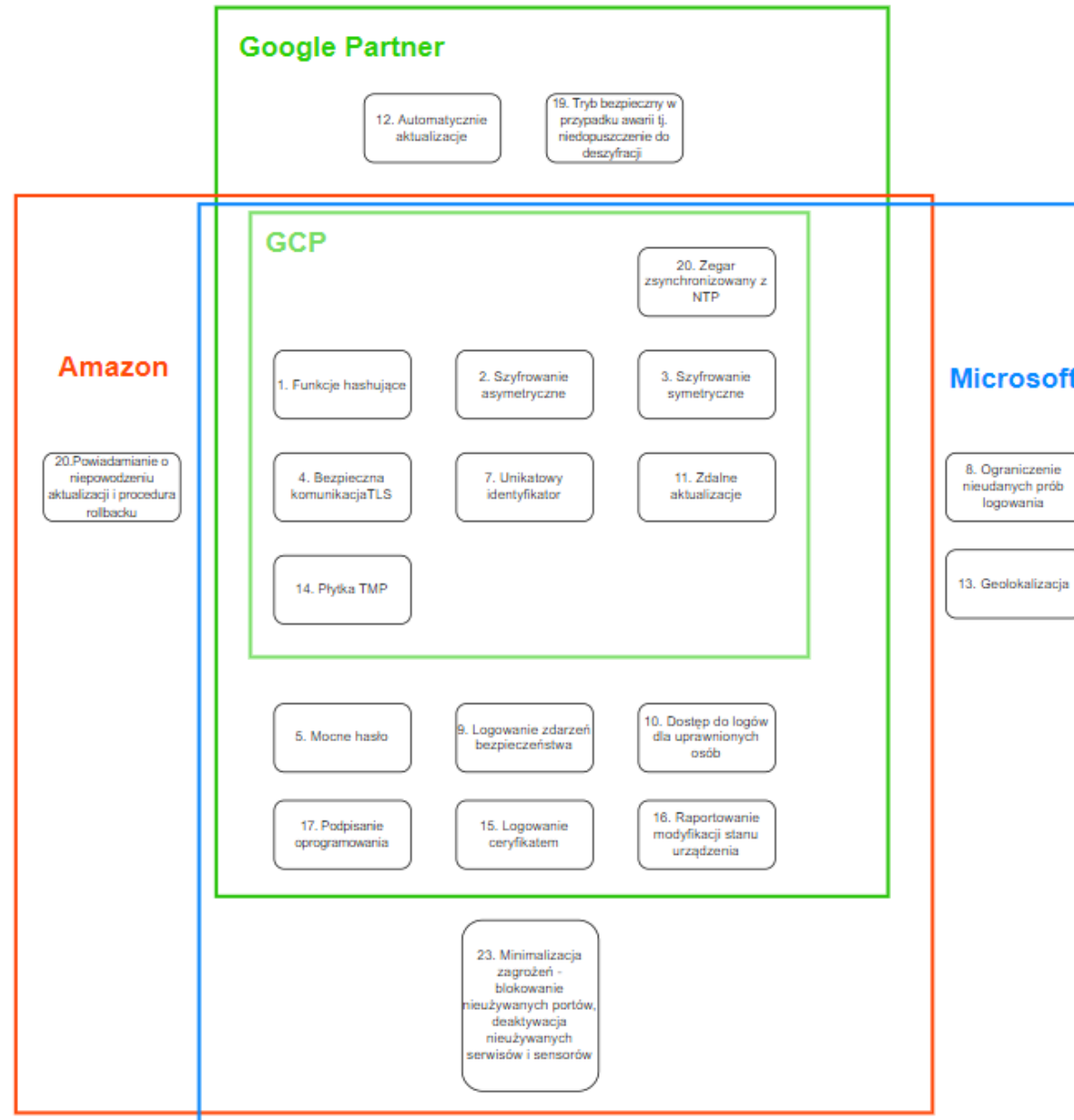
Teza pracy

Istnieje możliwość wyznaczenia idealnego węzła czujnikowego
i przekształcenia, pozwalającego określić poziom
bezpieczeństwa urządzeń Internetu Rzeczy

$$F(\text{cechy sensora rzeczywistego}) = \% \text{ zgodności}$$



Zbiory dostawców – wspólne



Wyznaczone poziomy bezpieczeństwa w kontekście zbiorów cech

Nr.	Opis	Dgoogle	Damazon	Dmicrosoft	Rnist	Renista	Amin	Asr	Azaw	Amax
1	Funkcje hashujące	X	X	X	X	X	X	X	X	X
2	Szyfrowanie asymetryczne	X	X	X	X	X	X	X	X	X
3	szyfrowanie symetryczne	X	X	X	X	X	X	X	X	X
4	Bezpieczna komunikacja TLS	X	X	X		X		X	X	X
5	Mocne hasło	X	X	X		X		X	X	X
6	Uwierzytelnianie wieloskładnikowe					X				X
7	Unikatowy identyfikator	X	X	X	X	X	X	X	X	X
8	Ograniczenie nieudanych prób logowania			X		X			X	X
9	Logowanie zdarzeń bezpieczeństwa	X	X	X	X	X	X	X	X	X
10	Dostęp do logów tylko dla uprawnionych osób	X	X	X	X	X	X	X	X	X
11	Zdalne aktualizowanie	X	X	X	X	X	X	X	X	X
12	Automatyczne aktualizacje	X			X	X			X	X
13	Geolokalizacja			X						X
14	Płytki TMP	X	X	X		X		X	X	X
15	Logowanie certyfikatem	X	X	X				X		X
16	Raportowanie modyfikacji stanu urządzenia	X	X	X		X		X	X	X
17	Podpisanie oprogramowania	X	X	X	X	X	X	X	X	X
18	Zegar zsynchronizowany z NTP	X								X
19	Tryb bezpieczny w przypadku awarii tj. niedopuszczenie do deszyfracji	X				X			X	X
20	Powiadomienie o niepowodzeniu aktualizacji i procedura rollbacku		X		X	X			X	X
21	Minimalizacja zagrożeń, blokowanie nieużywanych portów, deaktywacja nieużywanych serwisów i sensorów		X	X		X			X	X
22	Walidacja danych wejściowych					X				X

Minimalny poziom bezpieczeństwa

$$A_{min} = D_{google} \cap D_{amazon} \cap D_{microsoft} \cap R_{nist} \cap R_{renisa}$$

Nr	Cechy
1	Funkcje hashujące
2	Szyfrowanie asymetryczne
3	Szyfrowanie symetryczne
7	Unikatowy identyfikator
9	Logowanie zdarzeń bezpieczeństwa
10	Dostęp do logów tylko dla uprawnionych osób
11	Zdalne aktualizowanie
17	Podpisanie oprogramowania

Zbiór minimalny

1. Funkcje hashujące

2. Szyfrowanie
asymetryczne

3. Szyfrowanie
symetryczne

7. Unikatowy
identyfikator

9. Logowanie zdarzeń
bezpieczeństwa

10. Dostęp do logów
tylko dla uprawnionych
osób

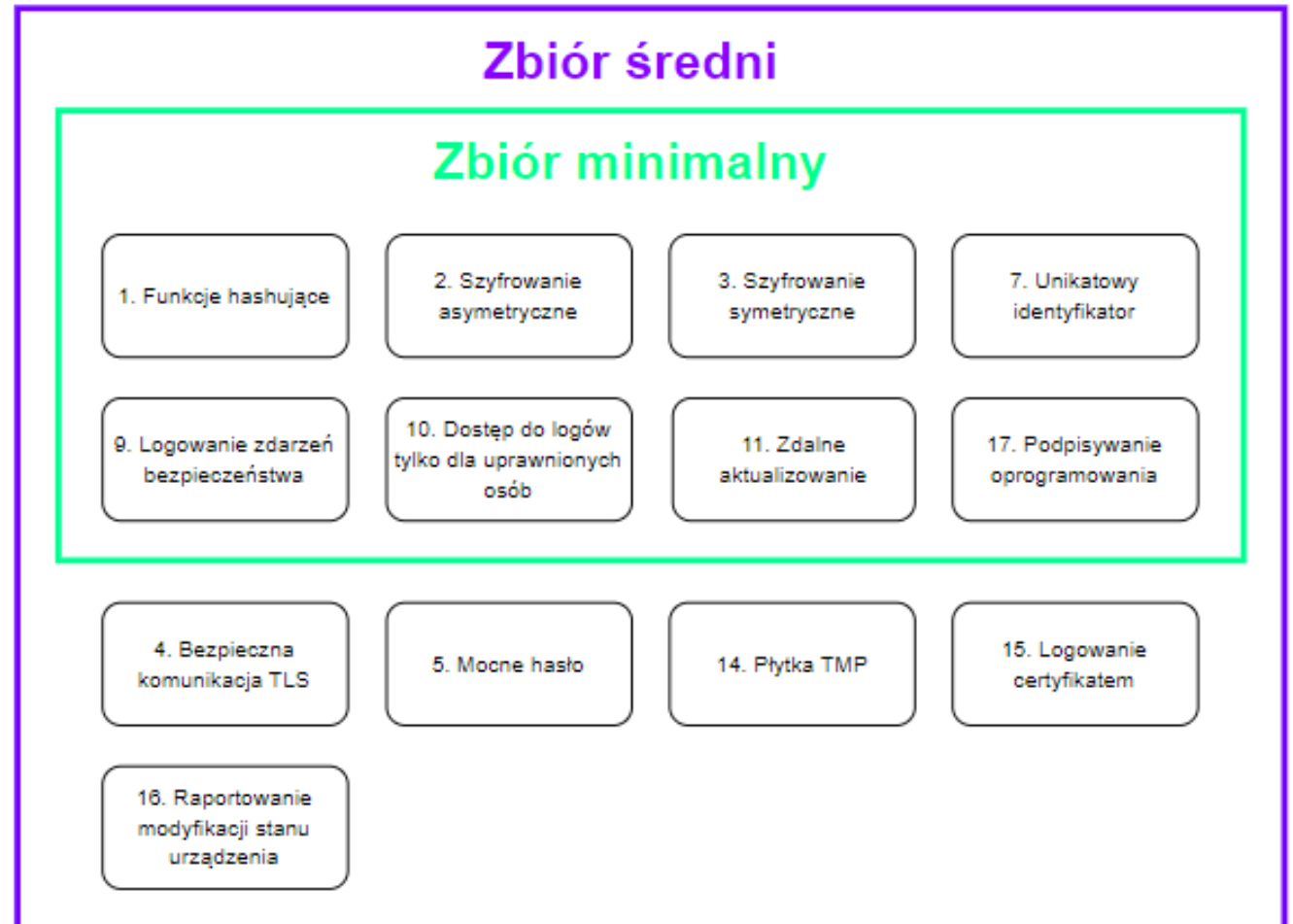
11. Zdalne
aktualizowanie

17. Podpisywanie
oprogramowania

Średni poziom bezpieczeństwa

$$A_{\text{śr}} = D_{\text{google}} \cap D_{\text{amazon}} \cap D_{\text{microsoft}}$$

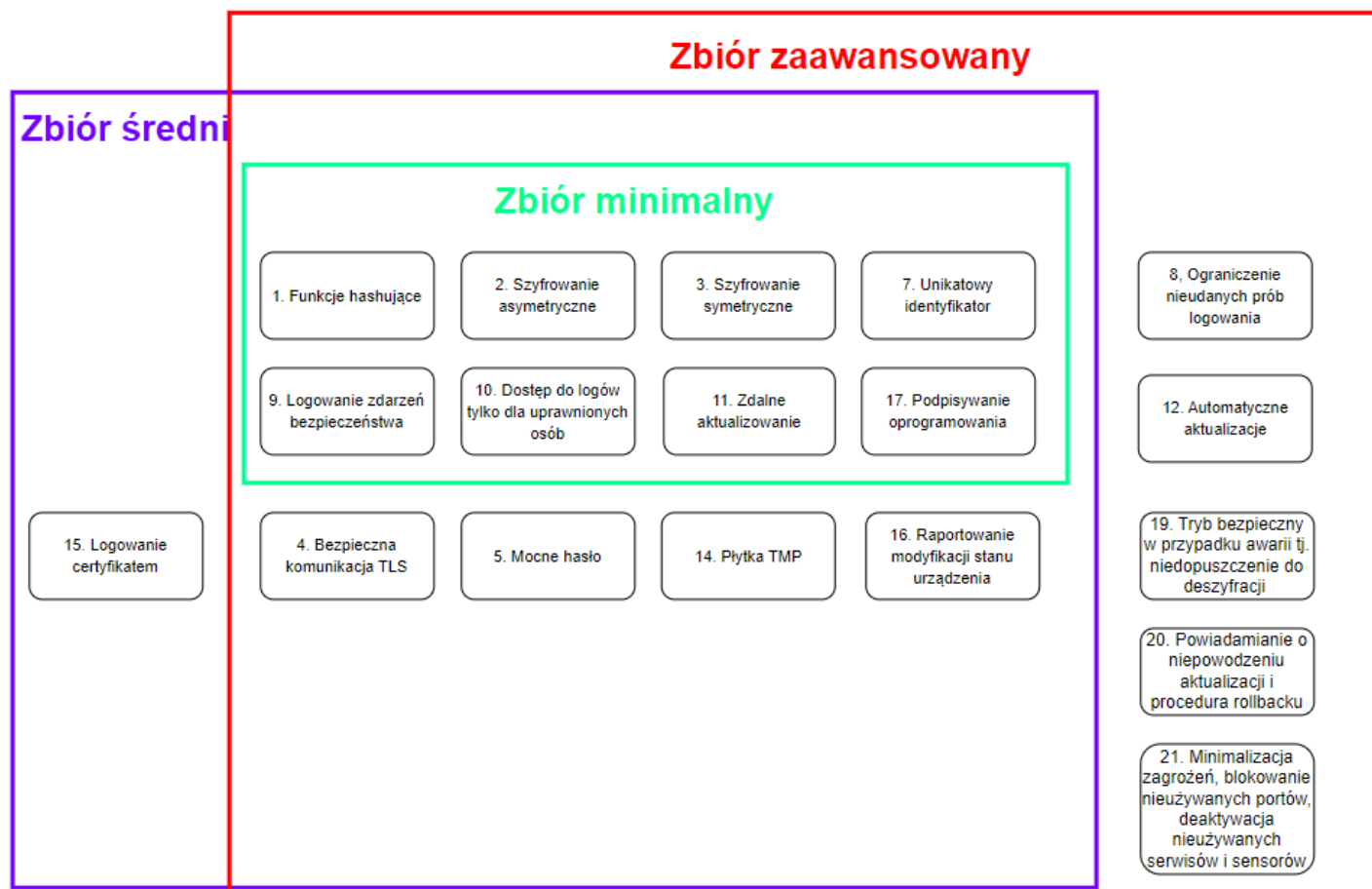
Nr	Cechy
1	Funkcje hashujące
2	Szyfrowanie asymetryczne
3	Szyfrowanie symetryczne
4	Bezpieczna komunikacja TLS
5	Mocne hasło
7	Unikatowy identyfikator
9	Logowanie zdarzeń bezpieczeństwa
10	Dostęp do logów tylko dla upoważnionych osób
11	Zdalne aktualizacje
14	Płytki TPM
15	Logowanie certyfikatem
16	Raportowanie modyfikacji stanu urządzenia
17	Podpisywanie oprogramowania



Zaawansowany poziom bezpieczeństwa

$$Azaw = (Dgoogle \cup Damazon \cup Dmicrosoft) \cap (Rnist \cup Renisa)$$

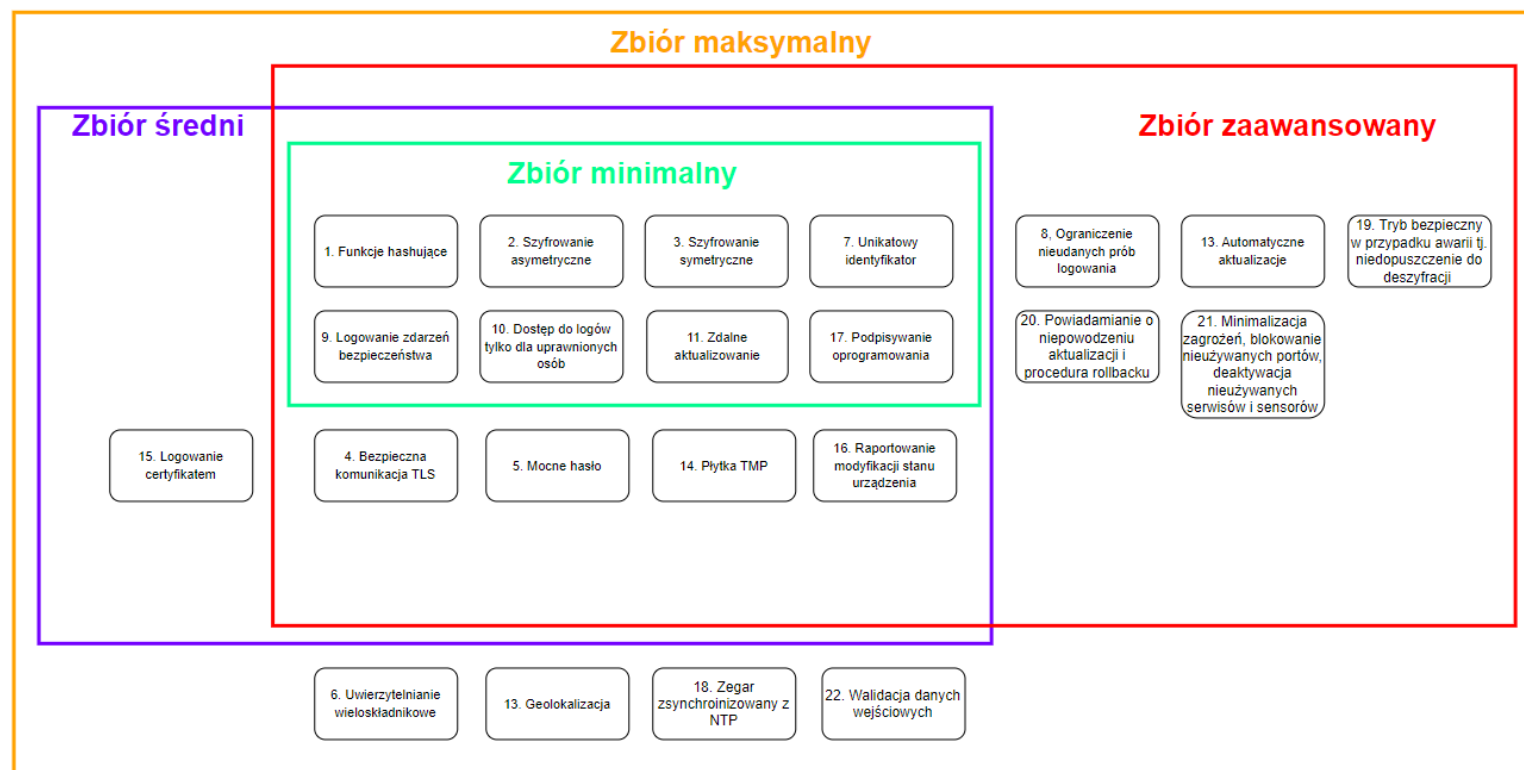
Nr	Cechy
1	Funkcje hashujące
2	Szyfrowanie asymetryczne
3	Szyfrowanie symetryczne
4	Bezpieczna komunikacja TLS
5	Mocne hasło
7	Unikatowy identyfikator
8	Ograniczenie nieudanych prób logowania
9	Logowanie zdarzeń bezpieczeństwa
10	Dostęp do logów tylko dla upoważnionych osób
11	Zdalne aktualizowanie
12	Automatyczne aktualizacje
14	Płytki TPM
16	Raportowanie modyfikacji stanu urządzenia
17	Podpisanie oprogramowania
19	Tryb bezpieczny w przypadku awarii tj. niedopuszczenie do deszyfracji
20	Powiadamanie o niepowodzeniu aktualizacji i procedura rollbacku
21	Minimalizacja zagrożeń, blokowanie nieużywanych portów, deaktywacja nieużywanych serwisów i sensorów



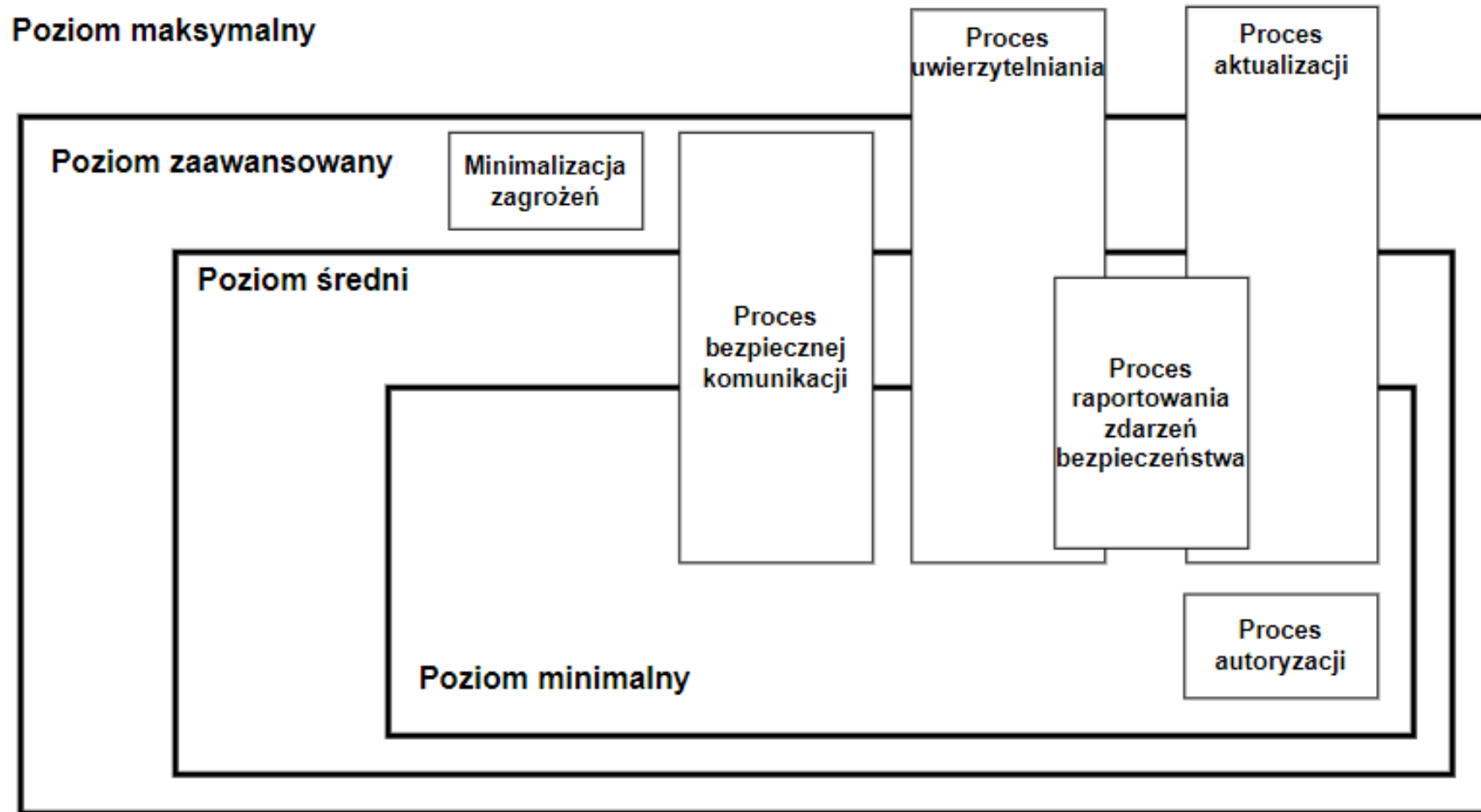
Maksymalny poziom bezpieczeństwa

$$A_{max} = D_{google} \cup D_{amazon} \cup D_{microsoft} \cup R_{nist} \cup R_{renisa}$$

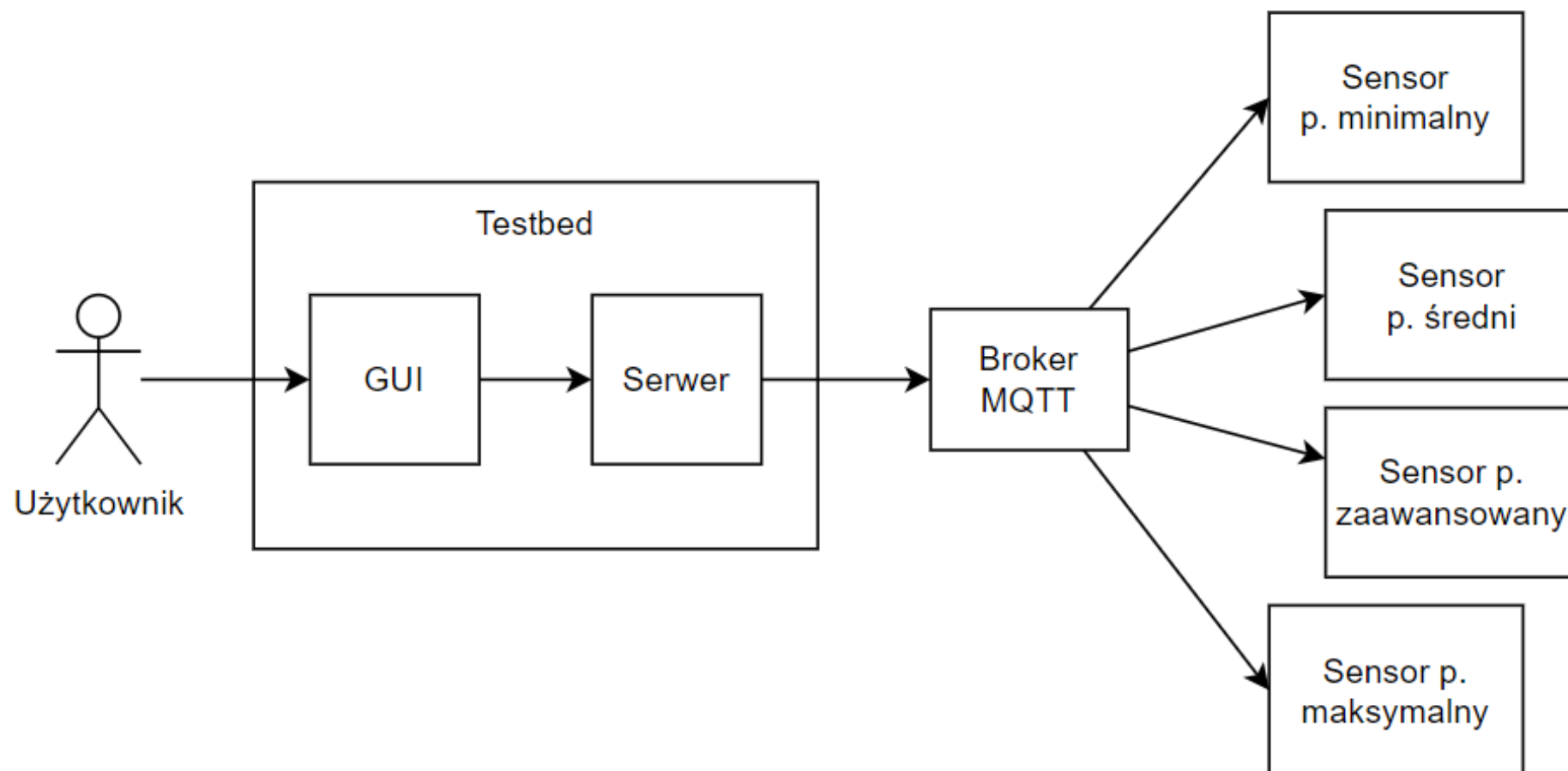
Nr	Cechy
1	Funkcje hashujące
2	Szyfrowanie asymetryczne
3	Szyfrowanie symetryczne
4	Bezpieczna komunikacja TLS
5	Mocne hasło
6	Uwierzytelnianie wieloskładnikowe
7	Unikatowy identyfikator
8	Ograniczenie nieudanych prób logowania
9	Logowanie zdarzeń bezpieczeństwa
10	Dostęp do logów tylko dla uprawnionych osób
11	Zdalne aktualizowanie
12	Automatyczne aktualizacje
13	Geolokalizacja
14	Płytki TPM
15	Logowanie certyfikatem
16	Raportowanie modyfikacji stanu urządzenia
17	Podpisanie oprogramowania
18	Zegar zsynchronizowany z NTP
19	Tryb bezpieczny w przypadku awarii tj. niedopuszczenie do deszyfracji
20	Powiadomienie o niepowodzeniu aktualizacji i procedura rollbacku
21	Minimalizacja zagrożeń, blokowanie nieużywanych portów, deaktywacja nieużywanych serwisów i sensorów
22	Walidacja danych wejściowych



Scenariusze użycia w kontekście poziomów bezpieczeństwa



Badania na testbedzie IoTrust - architektura



Lp.	Grupy testów	Testy	Sensor minimalny	Sensor średni	Sensor zaawansowany	Sensor maksymalny
1.1	Badanie uwierzytelniania	Blokada częstych logowań			X	X
1.2		Atak na uwierzytelnianie		X	X	X
1.3		Uwierzytelnianie dwupoziomowe				X
2.1	Badanie dostępności urządzenia		X	X	X	X
3.3		Próba aktualizacji plikiem z fałszywym podpisem SHA-2	X	X	X	X
3.7		Test przywrócenia poprzedniej wersji oprogramowania i konfiguracji			X	X
3.8		Badanie interwałów automatycznych aktualizacji			X	X
4.3		Poszukiwanie danych uwierzytelniania	X	X	X	X
4.4		Poszukiwanie usług i protokołów	X	X	X	X
4.6		Poszukiwanie zmian konfiguracji	X			
5.1	Badanie unikalnych identyfikatorów	Identyfikator logiczny	X	X	X	X
6.1.4		AES 128 CBC	X	X	X	X
6.1.5		AES 192 CBC		X	X	X
6.1.6		AES 256 CBC		X	X	X
6.2.3		RSA 2048	X	X	X	X
6.2.4		RSA 3072		X	X	X
9	Badanie dostępności interfejsów diagnostycznych			X	X	X

Rozwinięcie tezy

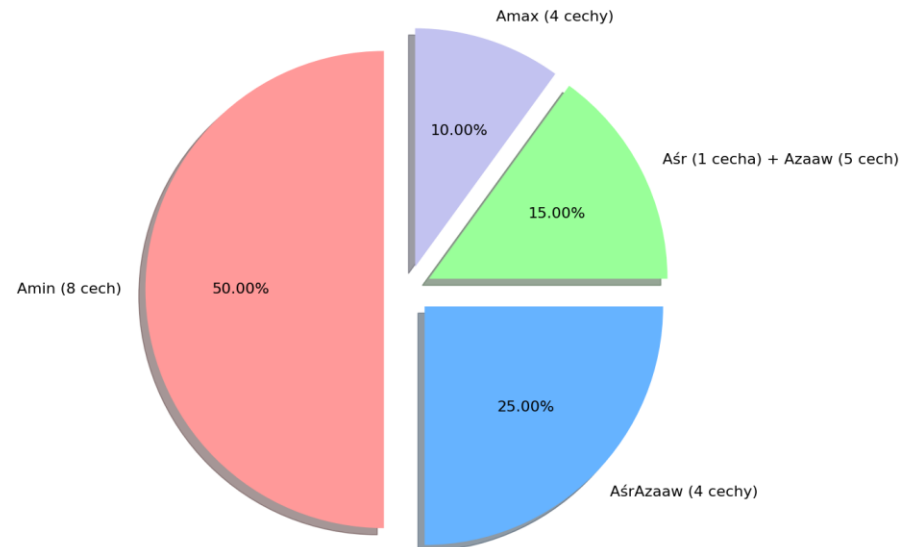
$F(\text{cechy sensora rzeczywistego}) =$

$$\left[w_{min} * \frac{x_{Amin}}{A_{min}} + w_{SrZaaw} * \frac{x_{A\acute{s}rAzaaw}}{(A_{\acute{s}r} \cap A_{zaaw}) \setminus A_{min}} + w_{\acute{s}r+zaaw} * \frac{x_{A\acute{s}r} + x_{Azaaw}}{(A_{\acute{s}r} \cup A_{zaaw}) \setminus (A_{\acute{s}r} \cap A_{zaaw})} + w_{max} * \frac{x_{Amax}}{A_{max} \setminus (A_{\acute{s}r} \cup A_{zaaw})} \right] * 100\%,$$

Współczynniki wagowe

$$w_{min} > w_{\acute{s}rZaaw} > w_{\acute{s}r+zaaw} > w_{max}$$

Proponowane wagi



- $w_{min} = \frac{1}{2}$
- $w_{\acute{s}rZaaw} = \frac{1}{4}$
- $w_{\acute{s}r+zaaw} = \frac{3}{20}$
- $w_{max} = \frac{1}{10}$

Autorskie osiągnięcia

- Wyznaczenie idealnego węzła IoT i określenie poszczególnych poziomów bezpieczeństwa.
- Zrzutowanie poziomów bezpieczeństwa na prawdziwe scenariusze użycia sensorów.
- Implementacja 4 symulatorów, odpowiadającym poszczególnym poziomom bezpieczeństwa i ich weryfikacja na testbedzie IoTTrust.
- Uwzględnienie w tezie poziomów bezpieczeństwa i ich wag.



Kierunki rozwoju

- Implementacja sprzętowa przedstawionych symulatorów
- Wyznaczenie nowych wag zbiorów

**Politechnika
Warszawska**

**Bezpieczny węzeł czujnikowy
oparty na IoT**

Praca dyplomowa magisterska

Maciej Krysiak

