

Uniwersalny wskaźnik analizy bezpieczeństwa urządzenia IoT

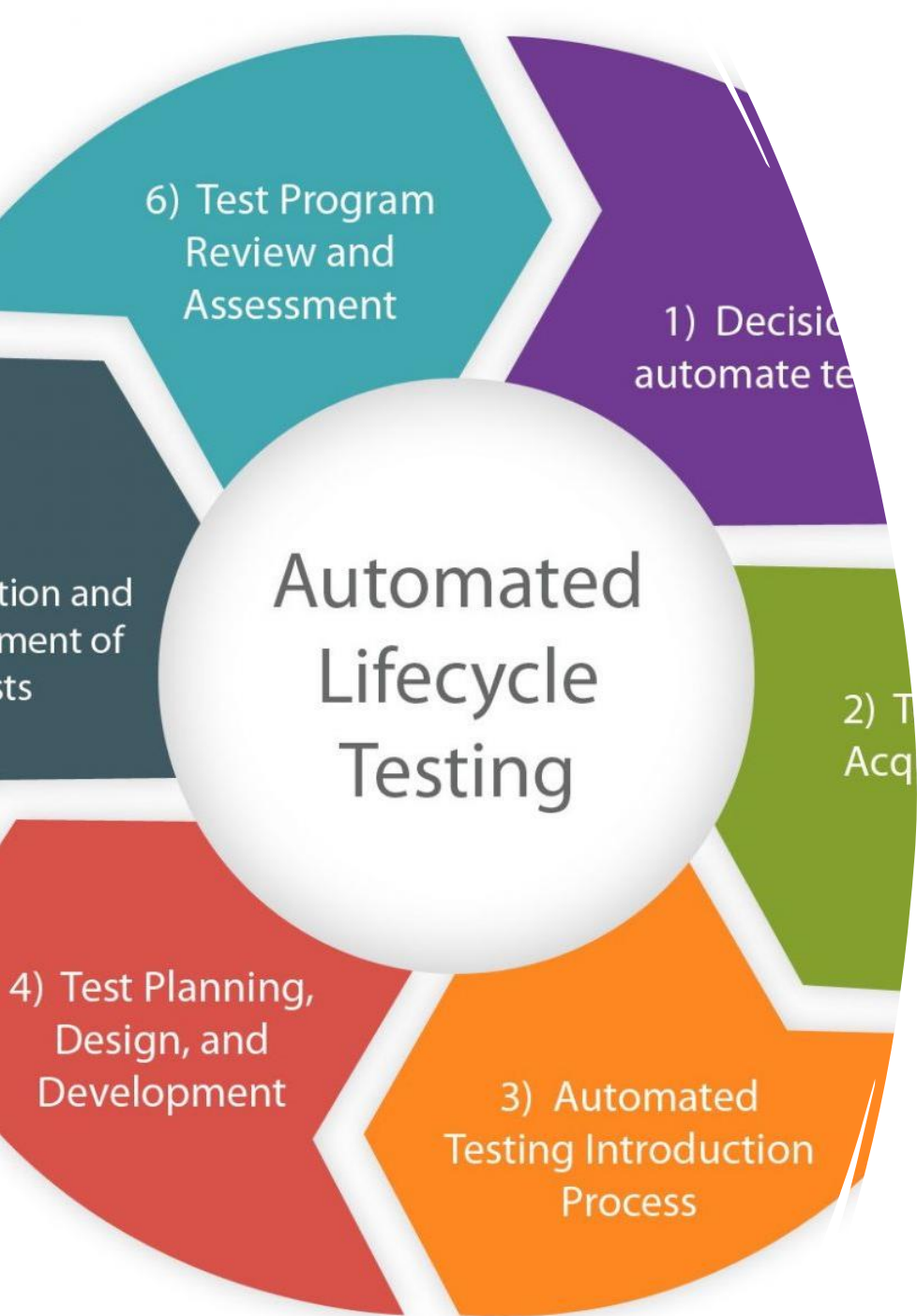
Łukasz Śleboda



Wstęp i Teza pracy

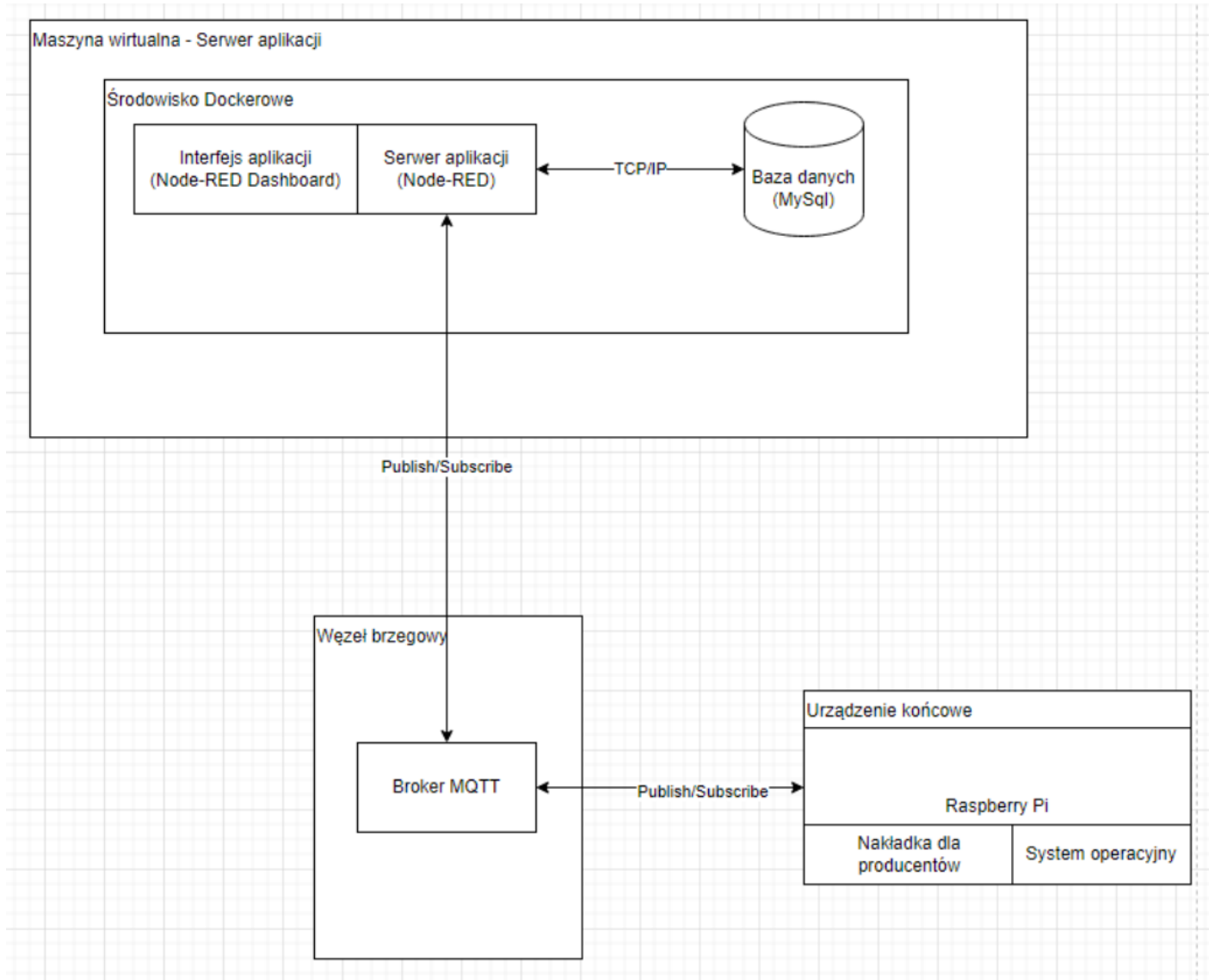
Możliwe jest opracowanie usystematyzowanych testów bezpieczeństwa dla urządzeń IoT i określenie, iż przy aktualnym stanie wiedzy możliwe jest przypisanie każdemu z testowanych urządzeń pewnego charakteryzującego go współczynnika jakościowego.



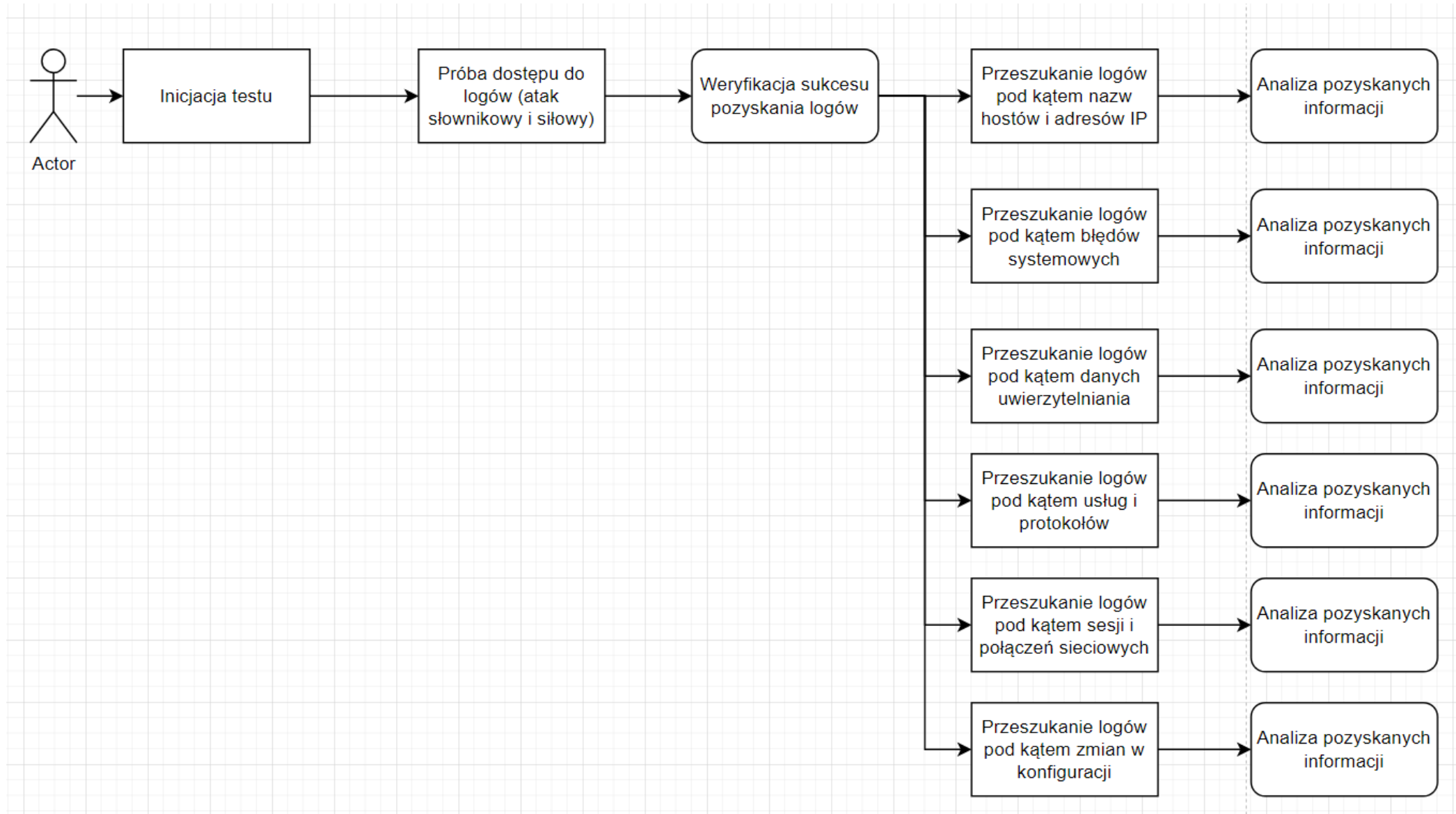


Projekt scenariuszy testowych

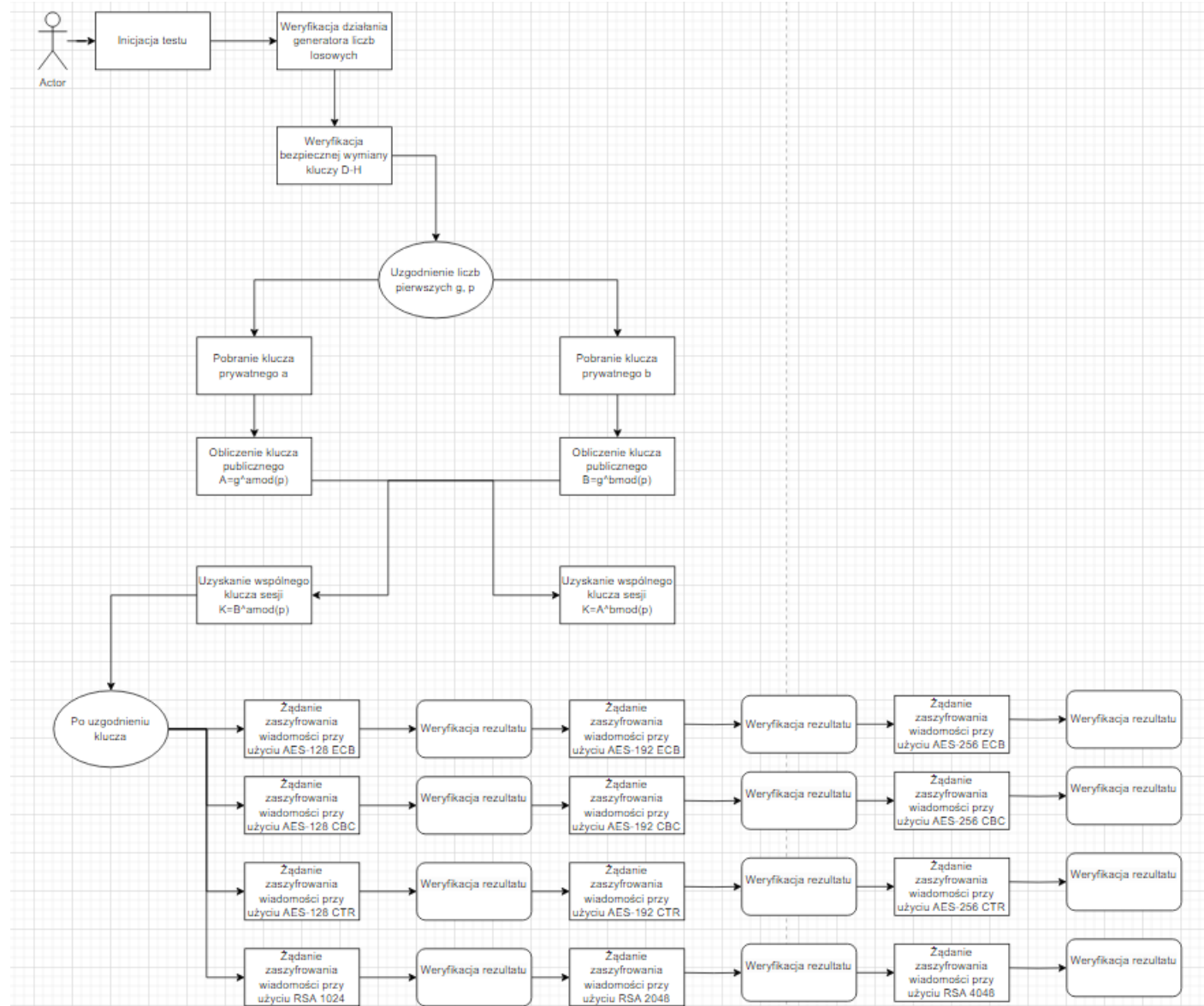
Architektura środowiska testowego

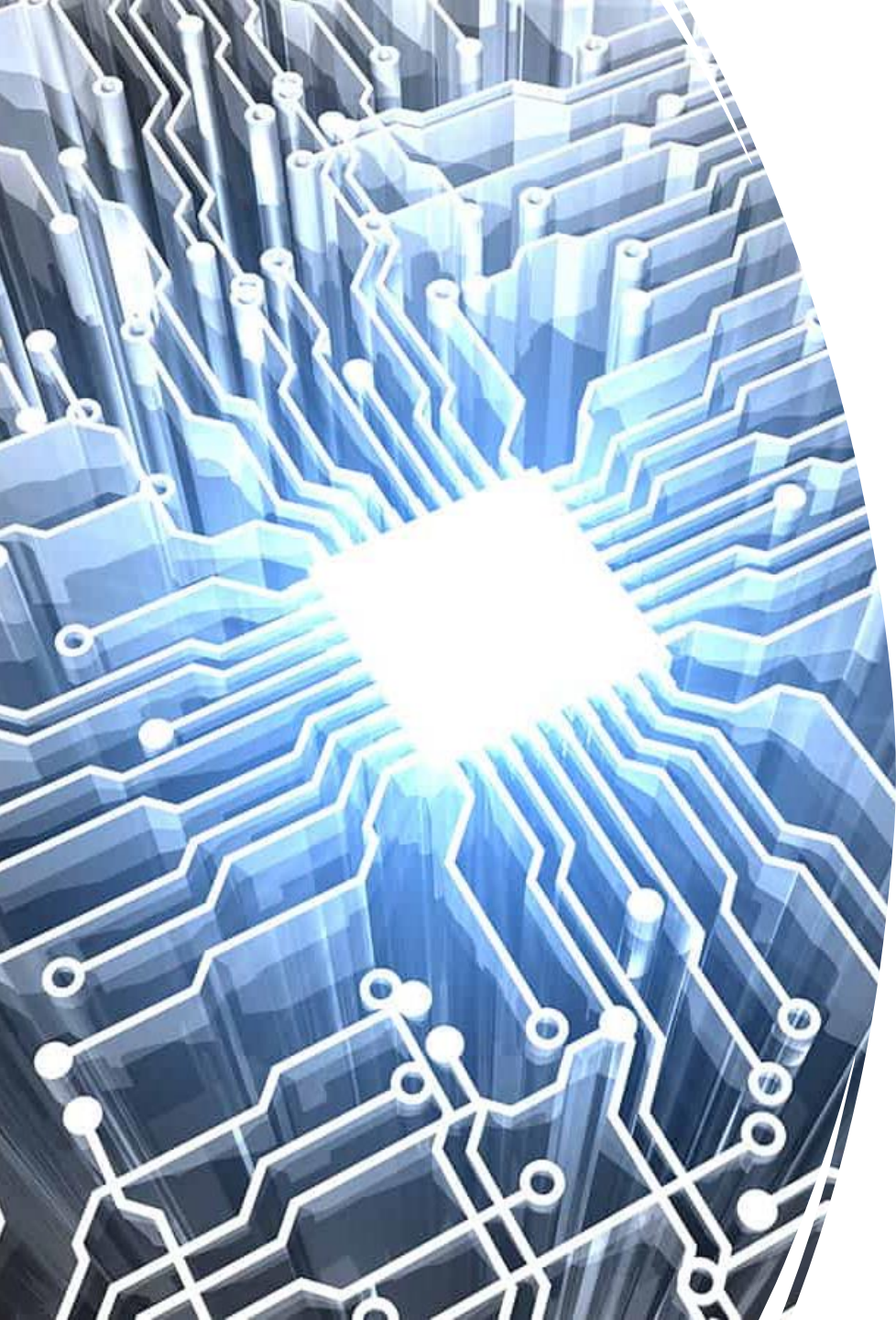


Przebieg scenariusza – Badanie logów



Przebieg scenariusza – Badanie algorytmów kryptograficznych





Wyznaczanie współczynnika jakości

Tabela cech w poszczególnych scenariuszach

	Badanie uwierzytelniania	Badanie dostępności urządzenia	Badanie aktualizacji	Badanie zawartości logów	Badanie unikalnych identyfikatorów	Badanie algorytmów kryptograficznych	Badanie zdolności przywrócenia oprogramowania i konfiguracji	Badanie szyfrowania nośnika danych	Badanie podziału pamięci operacyjnej	Badanie funkcjonalności automatycznej aktualizacji	Badanie dostępności interfejsów diagnostycznych	Badanie kontroli aktywnych połączeń
Procesor	0	X	X	0	0	X	0	0	0	0	0	0
Pamięć	0	X	X	0	0	X	0	0	0	0	0	0
Solidne hasło	X	0	X	X	X	X	0	0	0	0	X	0
Ograniczenie prób wielokrotnego logowania	X	0	0	X	0	0	0	0	0	0	0	0
Uwierzytelnianie dwuskładnikowe	X	0	X	X	0	0	0	0	0	0	0	0
MD5	0	0	X	0	0	0	0	0	0	0	0	0
SHA-1	0	0	X	0	0	0	0	0	0	0	0	0
SHA-2	0	0	X	0	0	0	0	0	0	0	0	0
SHA-3	0	0	X	0	0	0	0	0	0	0	0	0
RSA	X	0	X	0	0	X	X	0	0	0	0	0
AES	X	0	X	0	0	X	X	0	0	0	0	0
Ograniczony dostęp do logów	0	0	0	X	0	0	0	0	0	0	0	0

Tabela cech w poszczególnych scenariuszach

	Badanie uwierzytelniania	Badanie dostępności urządzenia	Badanie aktualizacji	Badanie zawartości logów	Badanie unikalnych identyfikatorów	Badanie algorytmów kryptograficznych	Badanie zdolności przywrócenia oprogramowania i konfiguracji	Badanie szyfrowania nośnika danych	Badanie podziału pamięci operacyjnej	Badanie funkcjonalności automatycznej aktualizacji	Badanie dostępności interfejsów diagnostycznych	Badanie kontroli aktywnych połączeń
Niebezpieczne informacje w logach	0	0	0	X	0	0	0	0	0	0	0	0
Unikalny identyfikator logiczny	X	0	0	X	X	0	X	0	0	0	0	0
Unikalny identyfikator fizyczny	0	0	0	0	X	0	0	0	0	0	0	0
Przywrócenie poprzedniej wersji oprogramowania	0	0	0	0	0	0	X	0	0	0	0	0
Przywrócenie poprzedniej wersji konfiguracji	0	0	0	0	0	0	X	0	0	0	0	0
Szyfrowanie nośnika danych	0	0	0	0	0	0	X	X	0	0	0	0
Podział pamięci operacyjnej	0	0	0	0	0	0	0	0	X	0	0	0
Aktualizacje automatyczne	0	0	0	0	0	0	0	0	0	X	0	0
Kontrola aktywnych połączeń	0	0	0	0	0	0	0	0	0	0	0	X
Dostępność urządzenia	0	X	0	0	0	0	0	0	0	X	0	0
Dostępność interfejsów diagnostycznych	0	0	X	X	0	0	0	0	0	0	X	0

Relacje pomiędzy
grupami
składającymi się
na węzeł IoT

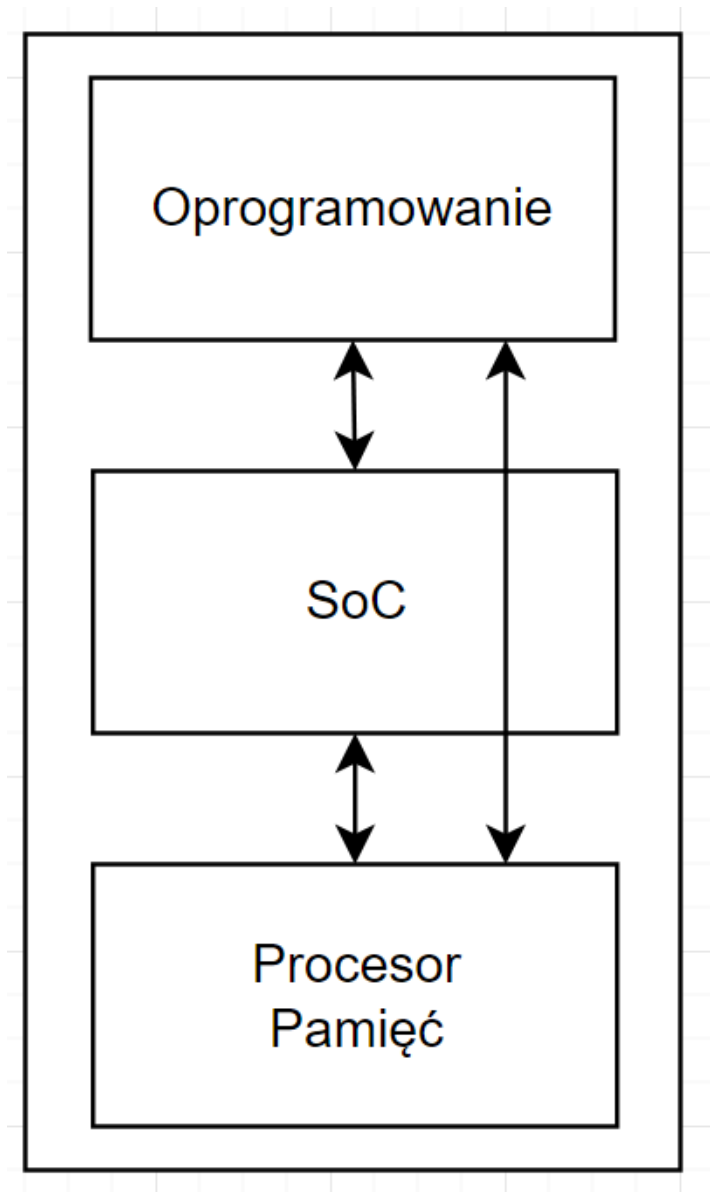


Tabela istotności cech dla danej grupy

	Procesor	Pamięć	Solidne hasło	Ograniczenie prób wielokrotnego logowania	Uwierzytelinianie dwuskładnikowe	MD5	SHA-1	SHA-2	SHA-3	RSA	AES	Ograniczony dostęp do logów	Niebezpieczne informacje w logach	Unikalny identyfikator logiczny	Unikalny identyfikator fizyczny	Przywrócenie poprzedniej wersji oprogramowania	Przywrócenie poprzedniej wersji konfiguracji	Szyfrowanie nośnika danych	Podział pamięci operacyjnej	Aktualizacje automatyczne	Kontrola aktywności połączeń	Dostępność urządzenia	Dostępność interfejsów diagnostycznych
Producent hardware	X	X										X			X			X				X	
Producent SoC				X	X	X	X	X	X	X	X												
Producent software			X	X	X									X		X	X	X		X	X		X

Tabela wag cech dla danej grupy

	Procesor	Pamięć	Solidne hasło	Ograniczenie prób wielokrotnego logowania	Uwierzytliwianie dwuskładnikowe	MD5	SHA-1	SHA-2	SHA-3	RSA	AES	Ograniczony dostęp do logów	Niebezpieczne informacje w logach	Unikalny identyfikator logiczny	Unikalny identyfikator fizyczny	Przywrócenie poprzedniej wersji oprogramowania	Przywrócenie poprzedniej wersji konfiguracji	Szyfrowanie nośnika danych	Podział pamięci operacyjnej	Aktualizacje automatyczne	Kontrola aktywności połączeń	Dostępność urządzenia	Dostępność interfejsów diagnostycznych
Producent hardware	40	40	5	5	5	5	5	5	5	5	5	20	5	5	20	5	5	20	5	5	5	10	5
Producent SoC	5	5	5	10	10	5	5	15	20	20	20	5	5	5	5	5	5	5	5	5	5	5	5
Producent software	5	5	40	30	30	5	5	5	5	5	5	5	5	30	5	20	20	20	5	20	20	5	20

Wyznaczanie współczynnika jakości - Q

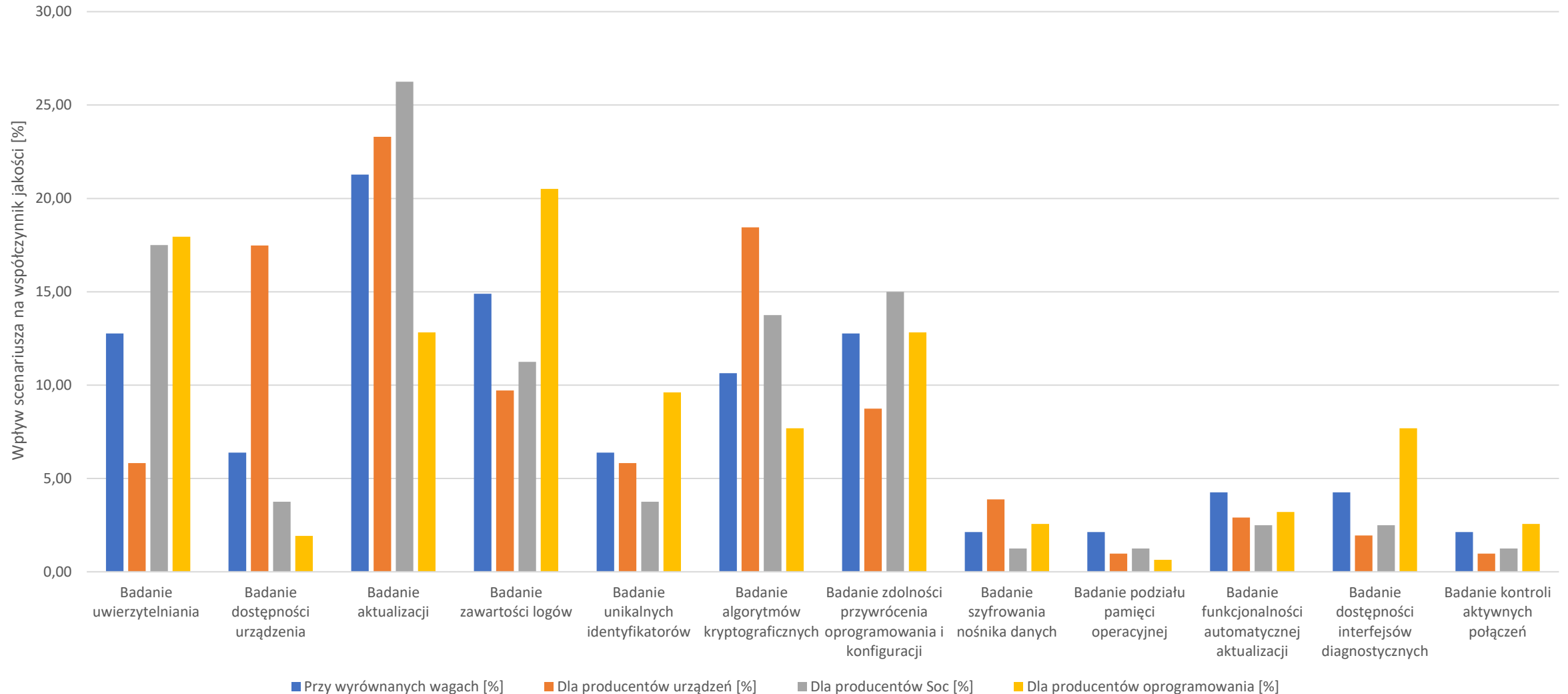
$$\sum_{i=1}^k Sw_i / Swc * 100\%$$

K – ilość scenariuszy testowych

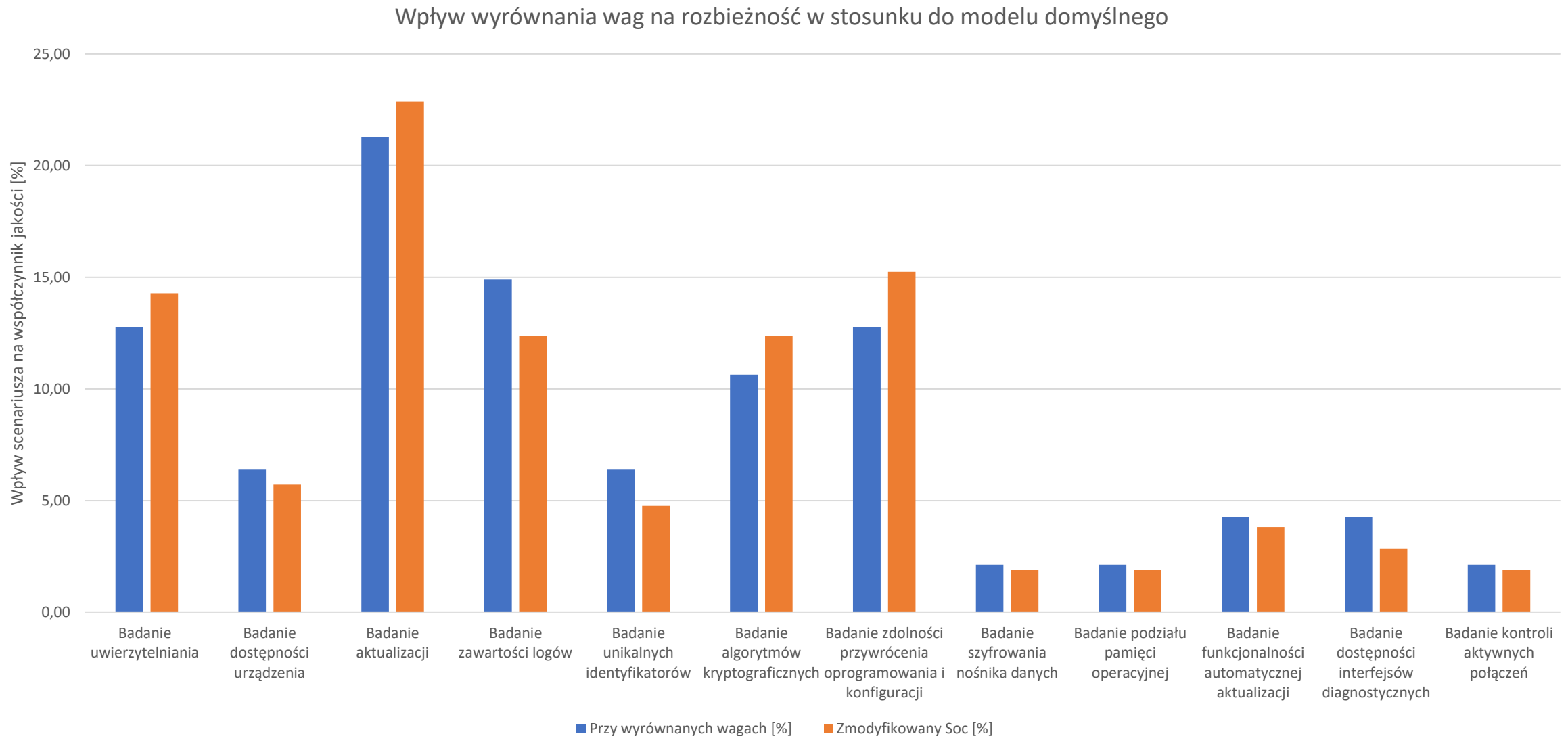
Swi – suma wag posiadanych cech i-tego scenariusza

Swc – suma wag wszystkich scenariuszy

Wpływ zmiany wagi cech na rozbieżność w stosunku do modelu domyślnego



Wpływ zmiany wagi cech na rozbieżność w stosunku do modelu domyślnego





Przeprowadzenie
badań w węźle
fizycznym

Wynik przeprowadzenia scenariusza - Badanie uwierzytelniania

	Blokada częstych logowań	Atak na uwierzytelnianie	Uwierzytelnianie dwupoziomowe
Sensor 1	-	-	-
Sensor 2	-	X	-
Sensor 3	X	X	-
Sensor 4	X	X	X

Wynik przeprowadzenia scenariusza - Badanie logów

	Poszukiwanie adresów IP i nazw hostów	Poszukiwanie błędów systemowych	Poszukiwanie danych uwierzytelniania	Poszukiwanie usług i protokołów	Poszukiwanie sesji i połączeń sieciowych	Poszukiwanie zmian konfiguracji
Sensor 1	-	-	X	X	-	X
Sensor 2	-	-	X	X	-	-
Sensor 3	-	-	X	X	-	-
Sensor 4	-	-	X	X	-	-

Wynik przeprowadzenia scenariusza - Badanie algorytmów kryptograficznych

	AES-128 CBC	AES-192 CBC	AES-256 CBC
Sensor 1	X	-	-
Sensor 2	X	X	X
Sensor 3	X	X	X
Sensor 4	X	X	X

Wnioski

Wydajność funkcji skrótu

Algorytm Blake2 okazał się jedynym, który pozwala na osiągnięcie najlepszej wydajności przy zachowaniu wysokiego poziomu bezpieczeństwa

Ograniczenia urządzeń IoT

Ze względów technicznych, takich jak ograniczone zasoby sprzętowe prostych urządzeń IoT nie jest możliwe technicznie zrealizowanie wszystkich zaleceń bezpieczeństwa

Zaniedbania producentów

Producenci urządzeń często zapominają o redundancji funkcji skrótu, kontroli aktywnych połączeń, szyfrowaniu pamięci urządzenia oraz zabezpieczenia interfejsów diagnostycznych

Możliwość określenia urządzeń przez współczynnik jakości

Po ustaleniu kluczowych dla danej grupy cech, możemy wyznaczyć współczynnik jakości Q dla każdego z testowanych urządzeń. Współczynnik ten jest sumą punktów zebranych w wyniku zaliczenia opracowanych scenariuszy testowych

Osiągnięcia

Projekt architektury i Realizacja systemu

Zaprojektowano,
zaimplementowano
oraz wdrożono
środowisko testowe dla
urządzeń IoT

Wyznaczenie sposobu na przypisanie urządzeniom współczynnika jakości

Wyznaczono metodę
określania poziomu
bezpieczeństwa
urządzeń poprzez
przypisywanie im
współczynnika jakości

Przeprowadzenie badań w węzłach IoT

Przeprowadzono
badania na węźle
fizycznym i
wystosowano
odpowiednie zalecenia
dla badanego
producenta

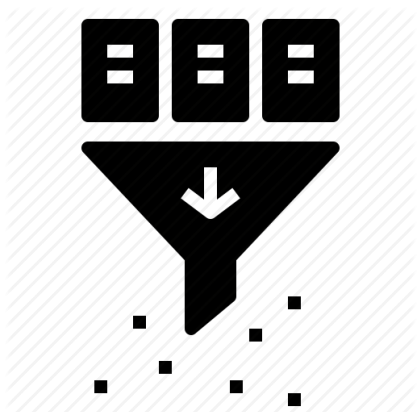
Wyznaczenie wytycznych bezpieczeństwa dla urządzeń iot

Określono wymagania
jakie powinno spełniać
idealne pod względem
bezpieczeństwa
urządzenie IoT

Zaprojektowanie scenariuszy testowych

Zaprojektowano i
zaimplementowano w
systemie scenariusze
testów bezpieczeństwa,
pozwalające na
identyfikację
ewentualnych słabości
w systemach IoT

Rozwój



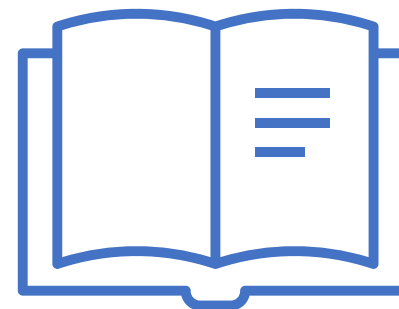
Nowe funkcje skrótu

Obsługa nowych funkcji skrótu pozwalających na jeszcze precyzyjniejsze określenie poziomu bezpieczeństwa



Nowe algorytmy kryptograficzne

Obsługa nowych algorytmów kryptograficznych pozwalających na spełnienie zapotrzebowania innych producentów urządzeń



Generacja raportów

Obsługa generacji raportów pozwoliłaby na lepszą analizę wyników testów bezpieczeństwa i ułatwiłaby dostęp do informacji o poziomie bezpieczeństwa dla użytkowników końcowych

Uniwersalny wskaźnik analizy bezpieczeństwa urządzenia IoT

Łukasz Śleboda

