



## POSUDEK VEDOUČÍHO DIPLOMOVÉ PRÁCE

**Jméno studenta:** Martin Šustr  
**Název práce:** Zabezpečení komunikace prvků IoT v prostředí smarthome  
**Autor posudku:** Mgr. Josef Horálek, Ph.D.  
**Cíl práce:** Cílem práce na provést analýzu, návrh a praktické ověření zabezpečení komunikace IoT prvků v prostředí smart home za využití komunikační technologie bluetooth nebo zigbee.

Povinná kritéria hodnocení práce	Stupeň hodnocení (známka)					
	A	B	C	D	E	F
Práce svým zaměřením odpovídá studovanému oboru	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vymezení cíle a jeho naplnění	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Zpracování teoretických aspektů tématu	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Zpracování praktických aspektů tématu	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Adekvátnost použitých metod, způsob jejich použití	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Hloubka a správnost provedené analýzy	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Práce s literaturou	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Logická stavba a členění práce	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Jazyková a terminologická úroveň	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Formální úprava a náležitosti práce	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vlastní přínos studenta	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Využitelnost výsledků práce v teorii (v praxi)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

### Vyjádření k výsledku anti-plagiátorské kontroly

Antiplagiátorská kontrola eVSKP identifikovala celkovou podobnost: 1 %.

### Dílní připomínky a náměty:

Vedoucí práce nemá závažné připomínky k předložené práci.

### Celkové posouzení práce a zdůvodnění výsledné známky:

V teoretické části práce autor analyzoval aktuální pohled na smart home s důrazem na problematiku jeho zabezpečení. Následně se zaměřil na podrobné představení technologií Bluetooth a ZigBee a analýzou jejich bezpečnostních zranitelností.

V praktické části autor představuje návrh řešení zabezpečení IoT prvků v prostředí smart home za využití vícevrstvé architektury, která zahrnuje koncové uzly, bránu smart home a RADIUS server. Základem navrženého mechanismu je ověření pomocí RADIUS serveru, sloužícího jako autentizační autorita a komunikujícího pouze s RADIUS klienty. Brána pak zajišťuje příjem autentizačních žádostí od koncových uzlů, přidává k žádosti další údaje, které jsou následně odeslané skrze RADIUS paket na RADIUS server. Základní princip autentizace pomocí RADIUS serveru je založen na sdíleném tajemství, které se neodesílá skrze síť. Tento princip byl ještě dále doplněn dalšími bezpečnostními mechanismy

s cílem co nejvíce mitigovat riziko neoprávněného přístupu. Navržené zabezpečení a další bezpečnostní mechanismy následně autor implementoval za využití malých a levných jednodeskových počítačů Raspberry Pi a platformy Arduino. Aplikace brány smart home byla implementovaná v jazyce Java s využitím frameworku Spring a poskytla grafické rozhraní implementované pomocí knihovny Swing. Realizované řešení pak bylo využito pro ověření funkčnosti navrženého konceptu zabezpečení. Pro ověření technologické nezávislosti, byly pro komunikaci mezi uzly a bránou využity technologie Bluetooth i ZigBee. Funkčnost samotného zabezpečení byla následně ověřena sadou testů, kdy byla ověřena autentizace, ovládání již autentizovaných uzlů a změna hesla. Odeslané RADIUS pakety byly ověřeny s využitím programu Wireshark. Práce splňuje požadavky kladené na diplomovou práci a doporučuji k obhajobě.

**Otázky k obhajobě:**

**Práci doporučuji k obhajobě.**

**Navržená výsledná známka: B**

**V Hradci Králové, dne 12. května 2021**

  
\_\_\_\_\_

**podpis**