TABLE IX

A SUMMARY OF THE SECURITY CONTROLS FOR IOT-ENABLED CYBER ATTACKS. FOR EACH CONTROL WE INDICATE THE MAIN THREAT AND/OR VULNERABILITY CHARACTERISTICS THAT ARE MITIGATED (AT LEAST PARTIALLY) BY THE CONTROL. WE ALSO INDICATE WHICH OF THE EXAMINED ATTACKS WOULD REQUIRE THIS SECURITY CONTROL, FOR ALL ATTACK PATHS

	Controlling Access				Mitigating IoT vulnerabilities													Examples of affected attack paths			Actor[a]
	Physical		Logical		HW layer			SW layer			Network & Protocols				Key Management						
SECURITY CONTROLS	Ins.	Out.	Priv.	Unpr.	Tamp-ering	Embed. Crypto	Implem-entation	Firm-ware	Operat. System	Applic-ation	Netw. Design	Link-Layer	Netw.-Layer	Appl.-Layer	No PKC	Common /No Key	Extract-able Key	Direct	Indirect	No conn.	
Limit physical access to IoT	✓				✓													[62], [165], [172], [175], [228]	[58], [83], [177]	[173], [229]	A
Monitor physical access to IoT	✓				✓													[62], [71], [111], [175]	[58], [83]	[229]	A
Avoid direct Internet access		✓	✓	✓					✓	✓			✓	✓	✓			[90], [92], [122], [138]	[179]	[12], [231], [233]	A
Enforce proxy-based access		✓	✓	✓					✓	✓				✓				[63], [90], [92], [111], [122], [138], [139], [165], [175], [228]	[57], [86]	[229], [233]	A
Secure remote access		✓	✓	✓									✓	✓				[63], [90], [92], [111], [122], [138], [139]	[57], [86], [179]	[12], [15], [233]	A
Apply security extensions for link-layer protocols	✓		✓	✓								✓						[145], [164], [165], [178], [198]	[144], [148]	[234]	A
Log and monitor access to IoT	✓	✓	✓	✓														[137]	[179], [180]	[12], [231]	A
Audit access to IoT	✓	✓	✓	✓															[179], [180]		A
Tamper resistance mechanisms	✓				✓	✓	✓	✓								✓	✓	[62], [111], [137], [145], [200]	[144]	[14]	M
Secure embedded crypto	✓	✓			✓	✓						✓	✓					[62], [122], [198]		[15]	M
Side-channel attack protection	✓				✓		✓													[15], [23], [230]	M
Firmware protection	✓	✓	✓	✓				✓										[62], [137], [138], [164], [200]	[57], [177]	[15]	M
Secure firmware update	✓							✓										[62], [164], [200]	[57], [177]	[15], [16], [230]	M
Secure OS architecture									✓									[63], [172], [178], [228]	[9], [10], [57], [58], [180], [209]	[12], [229], [230]	M
OS hardening									✓									[90], [172], [175], [178], [198]	[9], [10], [58], [180], [209]	[12], [229], [230]	M
Use of secure API										✓								[122], [138], [139], [177], [200]	[58], [83], [86], [146], [177]	[12], [14], [16], [23], [231], [233]	M
Code auditing										✓								[138], [139], [175], [200]	[58], [83], [86], [147], [177]	[14], [23], [231]	M
Network security protocols												✓	✓	✓				[111], [122], [145], [164], [165], [172]	[9], [10], [57], [144], [146], [147]	[23]	M
Secure key management																✓	✓	[172]	[177]	[14]–[16], [234]	M
Secure key exchange															✓	✓		[172]		[15], [16]	A
Device acquiring criteria					✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	[137], [175], [178], [198]		[233]	O
Secure change management						✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	[71], [172]	[58], [209]		A
Continuous security testing					✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	[178]	[9], [10], [209]	[12], [15], [230], [233], [234]	A
Security standards enforcement					✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	[145], [198]	[9], [10], [144], [147]	[12]	R
Identify IoT dependencies	✓	✓	✓	✓														[175]	[177], [180]	[16], [23], [173], [229]	A
Re-examine BYOD policies	✓		✓	✓																[14], [173]	A
Avoid physical proximity		✓	✓	✓															[83], [148]	[16], [23], [229], [230]	A
Segment networks to avoid cascading impact	✓	✓	✓	✓							✓							[71], [228]	[9], [10], [57], [58], [58], [146], [147], [177], [179], [180], [209]	[15]	A
Favor technology diversity	✓	✓	✓	✓							✓							[63]		[15]	O

[a] O: owner; A: administator; M: manufacturer; R: regulator