

# LIST OF FIGURES

1.1	Existing MQTT Scheme . . . . .	2
1.2	Existing MQTT Sequence . . . . .	2
2.1	Four-layers IoT [1] . . . . .	10
3.1	Seed and security attribute distribution . . . . .	34
3.2	Proposed connection phase . . . . .	36
3.3	Proposed authpublish phase . . . . .	37
3.4	Proposed secure protocol for MQTT . . . . .	39
3.5	The connection phase of the proposed method . . . . .	43
3.6	The authpublish phase of the proposed method . . . . .	45
4.1	Block diagram of validation protocol . . . . .	58
4.2	Executable existing registration phase MQTT protocol . . . . .	60
4.3	Packet sniffing existing registration phase MQTT protocol . . . . .	61
4.4	Executable existing registration phase MQTT protocol . . . . .	61
4.5	Packet sniffing existing publish phase MQTT protocol . . . . .	62
4.6	Executable proposed connection phase MQTT protocol 1 . . . . .	62
4.7	Executable proposed connection phase MQTT protocol 2 . . . . .	63
4.8	Packet sniffing proposed connection phase MQTT protocol 1 . . . . .	64
4.9	Packet sniffing proposed connection phase MQTT protocol 2 . . . . .	65
4.10	Packet sniffing proposed connection phase MQTT protocol 3 . . . . .	65
4.11	Packet sniffing proposed connection phase MQTT protocol 4 . . . . .	66
4.12	Authentication proposed connection phase MQTT protocol . . . . .	67
4.13	Mutual authentication proposed connection phase MQTT protocol . . . . .	67
4.14	Executable proposed authpublish phase MQTT protocol . . . . .	69
4.15	Packet sniffing proposed authpublish phase MQTT protocol . . . . .	70
4.16	Authentication proposed connection phase MQTT protocol . . . . .	70
5.1	Existing sequence . . . . .	73
5.2	Proposed sequence . . . . .	73
5.3	Microcontroller is able to process the proposed protocol . . . . .	79
5.4	Broker accept the client register . . . . .	80
5.5	Broker send authentication to the client . . . . .	81
5.6	Broker send mutual authentication . . . . .	81

5.7	Client receives mutual authentication . . . . .	81
5.8	Microcontroller send publish to the broker . . . . .	82
5.9	Broker receive publish from client . . . . .	82
5.10	Client publish package capture . . . . .	82
5.11	Broker send authentication to the client . . . . .	83
5.12	Client memory usage in the existing MQTT protocol . . . . .	85
5.13	Client memory usage in the proposed MQTT protocol in ESP8266-12 . . . . .	85
5.14	Client memory usage in the proposed MQTT protocol in Arduino Uno . . . . .	85
5.15	Real memory and CPU usage in existing MQTT protocol in registra- tion phase session 1 . . . . .	86
5.16	Real memory and CPU usage in existing MQTT protocol in publish phase session 1 . . . . .	87
5.17	Real memory and CPU usage in proposed MQTT protocol in connec- tion phase session 1 . . . . .	88
5.18	Real memory and CPU usage in proposed MQTT protocol in auth- publish phase session 1 . . . . .	89
5.19	Broker real memory and CPU usage in attack scenario session 1 . . . . .	89
A.1	Statistical Test . . . . .	100
A.2	Descriptive Statistics Test . . . . .	104
A.3	Attack Scenario . . . . .	105
A.4	Real memory and CPU usage in existing MQTT protocol in registra- tion phase session 2 . . . . .	106
A.5	Real memory and CPU usage in existing MQTT protocol in registra- tion phase session 3 . . . . .	106
A.6	Real memory and CPU usage in existing MQTT protocol in registra- tion phase session 4 . . . . .	107
A.7	Real memory and CPU usage in existing MQTT protocol in registra- tion phase session 5 . . . . .	107
A.8	Real memory and CPU usage in existing MQTT protocol in registra- tion phase session 6 . . . . .	108
A.9	Real memory and CPU usage in existing MQTT protocol in registra- tion phase session 7 . . . . .	108
A.10	Real memory and CPU usage in existing MQTT protocol in registra- tion phase session 8 . . . . .	109
A.11	Real memory and CPU usage in existing MQTT protocol in registra- tion phase session 9 . . . . .	109

A.12 Real memory and CPU usage in existing MQTT protocol in registration phase session 10 . . . . .	110
A.13 Real memory and CPU usage in existing MQTT protocol in publish phase session 2 . . . . .	111
A.14 Real memory and CPU usage in existing MQTT protocol in publish phase session 3 . . . . .	111
A.15 Real memory and CPU usage in existing MQTT protocol in publish phase session 4 . . . . .	112
A.16 Real memory and CPU usage in existing MQTT protocol in publish phase session 5 . . . . .	112
A.17 Real memory and CPU usage in existing MQTT protocol in publish phase session 6 . . . . .	113
A.18 Real memory and CPU usage in existing MQTT protocol in publish phase session 7 . . . . .	113
A.19 Real memory and CPU usage in existing MQTT protocol in publish phase session 8 . . . . .	114
A.20 Real memory and CPU usage in existing MQTT protocol in publish phase session 9 . . . . .	114
A.21 Real memory and CPU usage in existing MQTT protocol in publish phase session 10 . . . . .	115
A.22 Real memory and CPU usage in proposed MQTT protocol in connection phase session 2 . . . . .	116
A.23 Real memory and CPU usage in proposed MQTT protocol in connection phase session 3 . . . . .	116
A.24 Real memory and CPU usage in proposed MQTT protocol in connection phase session 4 . . . . .	117
A.25 Real memory and CPU usage in proposed MQTT protocol in connection phase session 5 . . . . .	117
A.26 Real memory and CPU usage in proposed MQTT protocol in connection phase session 6 . . . . .	118
A.27 Real memory and CPU usage in proposed MQTT protocol in connection phase session 7 . . . . .	118
A.28 Real memory and CPU usage in proposed MQTT protocol in connection phase session 8 . . . . .	119
A.29 Real memory and CPU usage in proposed MQTT protocol in connection phase session 9 . . . . .	119

A.30 Real memory and CPU usage in proposed MQTT protocol in connection phase session 10 . . . . .	120
A.31 Real memory and CPU usage in proposed MQTT protocol in verification phase session 2 . . . . .	121
A.32 Real memory and CPU usage in proposed MQTT protocol in verification phase session 3 . . . . .	121
A.33 Real memory and CPU usage in proposed MQTT protocol in verification phase session 4 . . . . .	122
A.34 Real memory and CPU usage in proposed MQTT protocol in verification phase session 5 . . . . .	122
A.35 Real memory and CPU usage in proposed MQTT protocol in verification phase session 6 . . . . .	123
A.36 Real memory and CPU usage in proposed MQTT protocol in verification phase session 7 . . . . .	123
A.37 Real memory and CPU usage in proposed MQTT protocol in verification phase session 8 . . . . .	124
A.38 Real memory and CPU usage in proposed MQTT protocol in verification phase session 9 . . . . .	124
A.39 Real memory and CPU usage in proposed MQTT protocol in verification phase session 10 . . . . .	125
A.40 Real memory and CPU usage in proposed MQTT protocol in attack scenario session 2 . . . . .	126
A.41 Real memory and CPU usage in proposed MQTT protocol in attack scenario session 3 . . . . .	126
A.42 Real memory and CPU usage in proposed MQTT protocol in attack scenario session 4 . . . . .	127
A.43 Real memory and CPU usage in proposed MQTT protocol in attack scenario session 5 . . . . .	127
A.44 Real memory and CPU usage in proposed MQTT protocol in attack scenario session 6 . . . . .	128
A.45 Real memory and CPU usage in proposed MQTT protocol in attack scenario session 7 . . . . .	128
A.46 Real memory and CPU usage in proposed MQTT protocol in attack scenario session 8 . . . . .	129
A.47 Real memory and CPU usage in proposed MQTT protocol in attack scenario session 9 . . . . .	129

A.48 Real memory and CPU usage in proposed MQTT protocol in attack  
scenario session 10 . . . . . 130