ABSTRACT

Internet of Things (IoT) connected devices will be reaching people seamlessly in future days. The security aspects for the IoT domain have always been open field of research and analysis. Each of the IoT protocols have its own strength and vulnerabilities. The Message Queue Telemetry Transport (MQTT) application layer IoT protocol is widely used in present day's context. Since, MQTT standard has no mandatory requirements regarding the security services; therefore, manipulating the security issues in MQTT platforms seems very easy. This thesis analyzes the security of MQTT protocol. Basing on the analysis, a security enhanced MQTT protocol is proposed. The proposed protocol is based with added cryptographic primitives to offer security services for IoT system. Mutual authentication between subscriber and broker, mutual authentication between publisher and broker, authentication with key distribution, use of only symmetric key cryptography are the few salient features of the proposed enhanced MQTT protocol. This thesis also conducts a formal verification for the proposed MQTT protocol to prove that the proposed protocol satisfies the intended security attributes. The evaluation result validates that the proposed protocol ensures the secrecy property of the cryptographic credentials and hence, operates securely.

ACKNOWLEDGEMENT

All appreciations are for the Almighty Allah for making me such eligible to take the effort and complete this research work.

The author would like to express his sincere gratitude to supervisor *Dr. Mohammed Shafiul Alam Khan, Associate Professor and Director, Institute of Information Technology (IIT) University of Dhaka* for his kind supervision, guidance, encouragement and inspection throughout the entire research period. The author also expresses thankful gratitude to Co-Supervisor *Lieutenant Colonel Dr. Muhammad Nazrul Islam, Instr Cl A, Department of Computer Science and Engineering, Military Institute of Science and Technology, Mirpur Cantonment* for his continuous support from the beginning of this thesis. Their kind cooperation and guidance made this thesis an effective one.

I would like to commend all the board members of Examiners for their valuable time in recognizing my work and their precious observations. I also thank all my friends and colleagues for their inspiration and advice. The author acknowledges Mr Jafor, for support during the field study.

TABLE OF CONTENTS

ABSTRACT **i**

ACKNOWLEDGEMENT **ii**

TABLE OF CONTENTS **iii**

LIST OF FIGURES **vi**

CHAPTER ONE : INTRODUCTION **1**

1.1 Background 1

1.2 Problem Statements 2

1.3 Thesis Objectives 2

1.4 Methodological Overview 3

1.5 Thesis Scope 3

1.6 Organization of the Thesis 4

CHAPTER TWO: THEORETICAL BACKGROUND AND RELATED WORKS **5**

2.1 Introduction to IoT Protocols 5

2.1.1 Security Aspects of IoT Protocol 7

2.1.2 Characteristics of IoT Protocols 7

2.2 An Overview of MQTT Protocol 8

2.3 Security Aspects of MQTT Protocol 9

2.4 Use of ProVerif 10

2.5 Critical Summary of Theoretical Studies 12

2.5 Related Works 12

2.5.1 Token Based Authentication 12

2.5.2 OAuth Approval Standards 14

2.5.3 Attribute Based Encryption (KP/CP ABE) 16

2.5.4 Use of Lightweight Cryptography 17

2.6 Summary of the Related Works 19

CHAPTER THREE : METHODOLOGY

3.1 Key Phases of Research Methodology 21

3.1.1 Identification of Research Questions 21

3.1.2 Design of modified protocol 22

3.1.3 Analysis of Protocol 22

3.2 Reference Publication Year and Types 23

3. 3. Steps followed in ProVerif 23

CHAPTER FOUR : ROPOSED SECURITY ENHANCED MQTT PROTOCOL

4.1 Authentication Server 24

4.2 Steps and Services 24

4.3 Authentication Pre-Processing Stage 25

4.4 Different Steps of Authentication 25

4.4 Key Features of the Proposed Protocol 28

CHAPTER FIVE : FORMAL MODELING FOR PROPOSED PROTOCOL

5.1 Procedure to be followed for using ProVerif Tool 29

5.2 Formal Model of the Proposed MQTT Scheme 30

5.2.1 The Declarations 31

5.2.2 The Process Macros 33

5.2.3 The Main Process 36

CHAPTER SIX : RESULT AND PERFORMANCE EVALUATION

6.1 ProVerif Verification Result 38

6.2 Analysis of the Proposed MQTT Protocol 40

6.2.1 Use of Symmetric Key Cryptography 40

6.2.2 Inclusion of Broker Authentication 40

6.2.3 Mutual Authentication between Broker and Publisher 41

6.2.4 Mutual Authentication between Broker and Subscriber 41

6.2.5 Authentication with Key Distribution 40

CHAPTER SEVEN : CONCLUSION AND FUTURE WORKS

7.1 Conclusion 42

7.2 Limitations and Future Work 43

REFERENCES **44**

APPENDIX A : PROVERIF CODES **A-1**

LIST OF FIGURES

Figure 2.1: Framework sequence – JWT 13

Figure 2.2: Authorization Mechanism in MQTT by OAuth Slandered 14

Figure 2.3: Sequence Diagram of the System Architecture of ECC 16

Figure 2.4: System Architecture with Lightweight cryptograph 18

Figure 3.1: Steps followed in Research Methodology 22

Figure 3.2: ProVerif Flow Diagram 23

Figure 4.1: Various Entity of the Proposed Protocol 24

Figure 4.2: Security Features of Proposed Model 25

Figure 4.3: Pre-processing Stage 26

Figure 4.4: Communication to Authentication Server through Broker. 27

Figure 4.5: Communication to Broker 27

Figure 4.6: Validating Broker 28

Figure 5.1: Summary of declaration - Enhanced MQTT Model 32

Figure 5.2: Client Process - Enhanced MQTT Model 34

Figure 5.3: Broker Process - Enhanced MQTT Model 35

Figure 5.4: Authentication Server Process - Enhanced MQTT Model 36

Figure 5.5: The Main process - Enhanced MQTT Model 37

Figure 6.1: MQTT protocol verification result - Session key secrecy 38

Figure 6.2: MQTT protocol verification result -User credential secrecy… 39

Figure 6.3: MQTT verification result - Broker credential secrecy 39