

PEOPLES' DEMOCRATIC REPUBLIC of ALGERIA  
Ministry of Higher Education and Scientific Research Ferhat  
Abbas University of Setif  
Faculty of Sciences



**MASTER THESIS**

**Domain: Computer Science Specialty:**  
**cyber security**

---

**Web-based management platform for secure key  
redistribution in IoT networks**

---

presented by:

**Issam Eddine HAMANI**

**Mahdi BENSLIM**

As a requirement to aim for the degree of  
Master in computer science

Supervisor:

Dr SAMI BETTAYEB

**Jury Members:**

Dr. Lakhdar GOUDJIL    President    University of Ferhat Abbas Setif 1

Dr. SKANDER HAMDI    Examiner    University of Ferhat Abbas Setif

# Abstract

Managing security keys for large, dynamic Internet of Things (IoT) networks is a significant challenge, often leading to security gaps and high operational costs. To address this, this project involved the design and implementation of a centralized web-based platform to simplify and automate this complex process. The platform is built upon a lightweight cryptographic method known as the Efficient Vectors-Based Key Management Scheme (EVKMS), which is specifically designed for resource-constrained devices. The system automates the entire security lifecycle of devices, including their addition, removal, and key updates, through a robust, task-based orchestration system managed by a modern backend server. A key contribution is the implementation of a comprehensive, immutable audit log that automatically records every administrative action, ensuring full traceability and accountability. The platform's effectiveness and its workflows were validated in a high-fidelity simulation environment that mimics real-world network communications. Ultimately, this work demonstrates that advanced security protocols can be successfully translated into practical, scalable, and user-friendly management tools for securing modern IoT deployments.

**keywords.** Internet of Things (IoT), Key Management, Security, EVKMS (Efficient Vectors-Based Key Management Scheme), Key Redistribution, Lifecycle Management, Web Platform, Automation, Simulation, Audit Log,

# Résumé

La gestion des clés de sécurité pour les vastes réseaux dynamiques de l'Internet des Objets (IoT) représente un défi majeur, entraînant souvent des failles de sécurité et des coûts opérationnels élevés. Pour y répondre, ce projet a consisté à concevoir et mettre en œuvre une plateforme web centralisée visant à simplifier et automatiser ce processus complexe. La plateforme s'appuie sur une méthode cryptographique légère, le « Efficient Vectors-Based Key Management Scheme » (EVKMS), spécialement conçue pour les appareils à ressources limitées. Le système automatise l'ensemble du cycle de vie de la sécurité des appareils, y compris leur ajout, leur suppression et la mise à jour de leurs clés, via un système d'orchestration robuste basé sur des tâches et géré par un serveur backend moderne. Une contribution essentielle est la mise en place d'un journal d'audit complet et immuable qui enregistre automatiquement chaque action administrative, garantissant une traçabilité et une responsabilité totales. L'efficacité de la plateforme et de ses flux de travail a été validée dans un environnement de simulation haute-fidélité reproduisant les communications d'un réseau réel. Enfin, ce travail démontre que des protocoles de sécurité avancés peuvent être traduits avec succès en outils de gestion pratiques, évolutifs et conviviaux pour sécuriser les déploiements IoT modernes.

## Mots-clés

Internet des objets (IoT), Gestion des clés, Sécurité, EVKMS (Schéma de gestion des clés basé sur des vecteurs efficaces), Redistribution des clés, Gestion du cycle de vie, Plateforme web, Automatisation, Simulation, Journal d'audit

تمثل إدارة مفاتيح السلامة للشبكات الديناميكية الواسعة لإنترنت الأشياء (IoT) تحديًا كبيرًا ، وغالبًا ما يتسبب في عيوب السلامة وتكاليف التشغيل المرتفعة. للإجابة عليه ، يتكون هذا المشروع في تصميم وتنفيذ منصة ويب مركزية تهدف إلى تبسيط هذه العملية المعقدة وأتمتة. يعتمد المنصة على طريقة تشفير خفيفة ، "مخطط إدارة المفاتيح القائم على المتجهات" (EVKMS) ، المصمم خصيصًا للموارد المحدودة. يقوم النظام بأتمتة دورة سلامة أجهزة أجهزة الحياة بأكملها ، بما في ذلك إضافتها وقمعها وتحديث مفاتيحها ، عبر نظام تزامن قوي يعتمد على المهام ويديره خادم الخلفية الحديث. تتمثل المساهمة الأساسية في تنفيذ مجلة تدقيق كاملة وغير متغيرة تسجل تلقائيًا كل إجراء إداري ، مما يضمن التتبع الكلي والمسؤولية. تم التحقق من صحة كفاءة المنصة وسير العمل في بيئة محاكاة عالية الدقة التي تستنسخ الاتصالات من شبكة حقيقية. أخيرًا ، يوضح هذا العمل أن بروتوكولات السلامة المتقدمة يمكن ترجمتها بنجاح إلى أدوات إدارة عملية وقابلة للتطوير وودية لتأمين عمليات نشر إنترنت الأشياء الحديثة.

### الكلمات الرئيسية

إنترنت الكائنات (IoT) ، الإدارة الرئيسية ، الأمن ، EVKMS (مخطط إدارة المفاتيح على أساس ناقلات فعالة) ، إعادة توزيع المفاتيح ، إدارة دورة الحياة ، منصة الويب ، الأتمتة ، المحاكاة ، مجلة التد



# Table of contents

|                                                              |            |
|--------------------------------------------------------------|------------|
| <b>Abstract</b>                                              | <b>i</b>   |
| <b>Table of contents</b>                                     | <b>ix</b>  |
| <b>List of figures</b>                                       | <b>x</b>   |
| <b>List of tables</b>                                        | <b>xi</b>  |
| <b>Abbreviations</b>                                         | <b>xii</b> |
| <b>Introduction</b>                                          | <b>1</b>   |
| <b>1 Background</b>                                          | <b>2</b>   |
| 1.1 Introduction .....                                       | 2          |
| 1.2 Internet of Things .....                                 | 2          |
| 1.2.1 IoT Definition .....                                   | 2          |
| 1.2.2 Applications of IoT .....                              | 4          |
| 1.2.3 Characteristics Of Iot .....                           | 7          |
| 1.2.4 Foundational IoT Architectures .....                   | 9          |
| 1.2.5 The Growing Importance of Interconnected Devices ..... | 11         |
| 1.3 Cyber Security (CS) with internet of things .....        | 11         |
| 1.3.1 Cybersecurity .....                                    | 11         |
| 1.3.2 Why we need Cs in iot ? .....                          | 12         |
| 1.3.3 Crucial Cyber Security Considerations for IoT .....    | 13         |
| 1.3.4 The most popular Attacks in iot .....                  | 14         |
| 1.3.5 IoT security principles .....                          | 16         |
| 1.4 Key Management Systems (KMS) .....                       | 17         |

|          |                                                                                   |           |
|----------|-----------------------------------------------------------------------------------|-----------|
| 1.4.1    | KMS Definition                                                                    | 18        |
| 1.4.2    | Key Management System Architecture                                                | 18        |
| 1.5      | Conclusion                                                                        | 20        |
| <b>2</b> | <b>Related Work</b>                                                               | <b>22</b> |
| 2.1      | Introduction                                                                      | 22        |
| 2.2      | Fundamentals of Cryptography and Key Management                                   | 23        |
| 2.2.1    | Symmetric and. Asymmetric Cryptography                                            | 23        |
| 2.2.2    | Key Lifecycle Management (Generation, Distribution, Storage, Revocation, refresh) | 2         |
|          | 4                                                                                 |           |
| 2.3      | Key Management Schemes In IoT And Wireless Sensor Networks                        | 25        |
| 2.3.1    | Definition                                                                        | 25        |
| 2.3.2    | Key Management Protocol For WSN                                                   | 26        |
| 2.3.3    | Cryptographic Schemes for WSNs                                                    | 27        |
| 2.3.4    | Static vs. Dynamic Key Management                                                 | 28        |
| 2.3.5    | Review of Specific KMS Protocols                                                  | 29        |
| 2.3.6    | Existing IoT Key Management Platforms and Tools                                   | 39        |
| 2.4      | Conclusion                                                                        | 40        |
| <b>3</b> | <b>The Efficient Vectors-Based Key Management Scheme (EVKMS)</b>                  | <b>42</b> |
| 3.1      | Introduction                                                                      | 42        |
| 3.2      | What Problem Does EVKMS Method Solve?                                             | 44        |
| 3.3      | Method Description                                                                | 44        |
| 3.3.1    | Network Model                                                                     | 44        |
| 3.3.2    | Key Management Phases                                                             | 44        |
| 3.4      | What Cryptographic Techniques Does It Use?                                        | 46        |
| 3.5      | Advantages                                                                        | 46        |
| 3.6      | Limitations                                                                       | 47        |
| 3.7      | Why This Method Was Chosen                                                        | 47        |
| 3.7.1    | Relevance for IoT                                                                 | 47        |
| 3.7.2    | Suitability for Web-Based Implementation                                          | 47        |
| 3.8      | Conclusion                                                                        | 48        |

|          |                                                            |           |
|----------|------------------------------------------------------------|-----------|
| <b>4</b> | <b>Design and Implementation of the Web Platform</b>       | <b>49</b> |
| 4.1      | Introduction                                               | 49        |
| 4.2      | Objectives of the Platform                                 | 50        |
| 4.3      | System Architecture                                        | 50        |
| 4.3.1    | Core Components                                            | 51        |
| 4.3.2    | Database Schema and Security Model                         | 54        |
| 4.4      | Operational Workflows and Data Flow                        | 55        |
| 4.5      | Key Functionalities                                        | 59        |
| 4.5.1    | Centralized Device and Network Management                  | 60        |
| 4.5.2    | Task-Based Key Lifecycle Orchestration                     | 60        |
| 4.5.3    | Autonomous Pairwise Key Establishment                      | 60        |
| 4.5.4    | Secure Storage and Auditing                                | 61        |
| 4.5.5    | Automated and Manual Key Rotation                          | 61        |
| 4.5.6    | Simulation Environment                                     | 61        |
| 4.6      | Technologies Used                                          | 63        |
| 4.6.1    | Frontend Technologies (Administrative Dashboard)           | 63        |
| 4.6.2    | Backend Technologies                                       | 64        |
| 4.6.3    | Database Technologies                                      | 65        |
| 4.6.4    | Containerization                                           | 66        |
| 4.6.5    | Messaging Protocol                                         | 66        |
| 4.6.6    | Development IDE                                            | 66        |
| 4.7      | Screenshots or Interface Walkthrough                       | 67        |
| 4.7.1    | Dashboard Overview:                                        | 67        |
| 4.7.2    | Network Topology Management (Subsets, Gateways, Devices) . | 67        |
| 4.7.3    | Task Orchestration and Monitoring                          | 68        |
| 4.7.4    | Security Auditing                                          | 69        |
| 4.8      | Conclusion                                                 | 70        |
|          | <b>Conclusion</b>                                          | <b>72</b> |
|          | <b>Bibliography</b>                                        | <b>73</b> |