

**Faculty of Engineering – Ain Shams University**

Computer and Systems Engineering Department

# **zGate Gateway: A Zero Trust Database Access Proxy**

Graduation Project Thesis

**Team Members:**

Michael George

Karen ...

Rodina ...

**Supervisor:**

Dr. ...

Academic Year 2025–2026

## **Acknowledgments**

We would like to thank...

## **Abstract**

This project introduces a Zero Trust–based database access gateway (SecureDB Gateway)...

# Contents

<b>1 Team Information</b>	<b>7</b>
1.1 Team Members . . . . .	7
1.2 Roles & Responsibilities . . . . .	7
<b>2 Introduction &amp; Problem Definition</b>	<b>8</b>
2.1 Introduction . . . . .	8
2.2 Problem Statement . . . . .	8
2.3 Gap in Existing Solutions . . . . .	8
2.4 Why Zero Trust for Databases is Different . . . . .	8
<b>3 Project Definition</b>	<b>9</b>
3.1 Project Definition & Scope . . . . .	9
3.2 Objectives . . . . .	9
3.3 Expected Academic Contribution . . . . .	9
<b>4 Requirements Engineering</b>	<b>10</b>
4.1 Functional Requirements . . . . .	10
4.2 Non-Functional Requirements . . . . .	10
4.3 Actors & Use Cases . . . . .	10
4.4 Use Case Diagrams . . . . .	10
4.5 User Stories . . . . .	10
<b>5 Proposed Solution</b>	<b>11</b>
5.1 Overview of the Proposed Solution . . . . .	11
5.2 Solution Architecture Layers . . . . .	11
5.2.1 Authentication Layer . . . . .	11
5.2.2 Proxy Layer . . . . .	11
5.2.3 Policy Engine Layer . . . . .	11
5.2.4 Data Protection Layer . . . . .	11
5.2.5 Observability Layer . . . . .	11
5.3 Term 1 vs Term 2 Features . . . . .	11
5.4 Feature List . . . . .	11

<b>6 Alignment with International Standards</b>	<b>12</b>
6.1 PCI DSS . . . . .	12
6.2 HIPAA . . . . .	12
6.3 GDPR . . . . .	12
6.4 ISO 27001 . . . . .	12
<b>7 Competitor &amp; Market Analysis</b>	<b>13</b>
7.1 Competitor Analysis . . . . .	13
7.1.1 Comparison Table . . . . .	13
7.1.2 What Competitors Lack . . . . .	13
7.2 Market Research . . . . .	13
7.2.1 Market Overview . . . . .	13
7.2.2 Zero Trust Demand . . . . .	13
7.2.3 Market Challenges & Needs . . . . .	13
7.2.4 Regulatory Drivers . . . . .	13
7.2.5 Trends & Opportunities . . . . .	13
7.2.6 Landscape Summary . . . . .	13
<b>8 Scientific Research &amp; Literature Review</b>	<b>14</b>
8.1 Paper 1 . . . . .	14
8.2 Paper 2 . . . . .	14
8.3 Paper 3 . . . . .	14
8.4 Paper 4 . . . . .	14
8.5 Paper 5 . . . . .	14
8.6 Paper 6 . . . . .	14
8.7 Paper 7 . . . . .	14
<b>9 System Architecture</b>	<b>15</b>
9.1 High-Level Architecture Diagram . . . . .	15
9.2 Main System Components . . . . .	15
9.3 Component Communication Flow . . . . .	15
9.4 Tech Stack Summary . . . . .	15
<b>10 Detailed Architecture of the Proxy</b>	<b>16</b>
10.1 Connection Lifecycle . . . . .	16
10.2 Authentication Flow . . . . .	16
10.3 Query Filtering Flow . . . . .	16
10.4 Policy Enforcement Flow . . . . .	16
10.5 Session Monitoring Flow . . . . .	16
10.6 User → Gateway → Database Diagram . . . . .	16

<b>11 High-Level Data Flow Diagrams</b>	<b>17</b>
11.1 Authentication Flow Diagram . . . . .	17
11.2 Query Filtering Diagram . . . . .	17
11.3 Logging & Auditing Flow Diagram . . . . .	17
<b>12 Technology Justification</b>	<b>18</b>
12.1 Why Go . . . . .	18
12.2 Why Node.js / TS / React . . . . .	18
12.3 Why mTLS (and why TCP is temporary) . . . . .	18
12.4 Why SQLite / Internal Storage . . . . .	18
12.5 Design Decision Summary . . . . .	18
<b>13 Prototype – Semester 1</b>	<b>19</b>
13.1 Implemented Features . . . . .	19
13.2 Screenshots (CLI & Dashboard) . . . . .	19
13.3 What Works vs What Doesn't . . . . .	19
13.4 Technical Decisions Made . . . . .	19
13.5 Implementation Challenges . . . . .	19
<b>14 Development Methodology</b>	<b>20</b>
14.1 Agile Method . . . . .	20
14.2 Meeting Structure . . . . .	20
14.3 Collaboration Tools . . . . .	20
14.4 Documentation & Observability . . . . .	20
<b>15 Task Tracking</b>	<b>21</b>
15.1 Team Task Tracking (Actual Examples) . . . . .	21
15.2 Supervisor Tracking Logs . . . . .	21
15.3 Blockers, Risks & Resolution Notes . . . . .	21
<b>16 Milestones</b>	<b>22</b>
16.1 Term 1 Milestone Roadmap . . . . .	22
16.1.1 Milestone 1 . . . . .	22
16.1.2 Milestone 2 . . . . .	22
16.1.3 Milestone 3 . . . . .	22
16.1.4 Milestone 4 . . . . .	22
16.1.5 Milestone 5 . . . . .	22
16.2 Timeline Chart (Gantt-like) . . . . .	22
<b>17 Threat Model &amp; Security Considerations</b>	<b>23</b>
17.1 Threat Model . . . . .	23

17.2 Risks & Attack Vectors . . . . .	23
17.3 Mitigation Techniques . . . . .	23
17.4 Why Zero Trust is Needed . . . . .	23
<b>18 Roadmap for Term 2</b>	<b>24</b>
18.1 Remaining Features . . . . .	24
18.2 Architecture Improvements . . . . .	24
18.3 Performance Goals . . . . .	24
18.4 Testing & Validation Plan . . . . .	24
<b>19 Team Contribution</b>	<b>25</b>
19.1 Overview of Contribution Approach . . . . .	25
19.2 Individual Contributions . . . . .	25
<b>20 Expected Outcomes</b>	<b>26</b>
<b>21 Conclusion</b>	<b>27</b>
21.1 Restated Purpose . . . . .	27
21.2 Summary of Achievements . . . . .	27
21.3 Importance & Contribution . . . . .	27
21.4 Transition to Next Semester . . . . .	27
<b>A Glossary</b>	<b>29</b>
<b>B Dashboard Mockups</b>	<b>30</b>

## List of Figures

## List of Tables

## **1. Team Information**

### **1.1 Team Members**

### **1.2 Roles & Responsibilities**

## **2. Introduction & Problem Definition**

### **2.1 Introduction**

### **2.2 Problem Statement**

### **2.3 Gap in Existing Solutions**

### **2.4 Why Zero Trust for Databases is Different**

### **3. Project Definition**

#### **3.1 Project Definition & Scope**

#### **3.2 Objectives**

#### **3.3 Expected Academic Contribution**

## **4. Requirements Engineering**

### **4.1 Functional Requirements**

### **4.2 Non-Functional Requirements**

### **4.3 Actors & Use Cases**

### **4.4 Use Case Diagrams**

### **4.5 User Stories**

## **5. Proposed Solution**

### **5.1 Overview of the Proposed Solution**

### **5.2 Solution Architecture Layers**

#### **5.2.1 Authentication Layer**

#### **5.2.2 Proxy Layer**

#### **5.2.3 Policy Engine Layer**

#### **5.2.4 Data Protection Layer**

#### **5.2.5 Observability Layer**

### **5.3 Term 1 vs Term 2 Features**

### **5.4 Feature List**

## **6. Alignment with International Standards**

**6.1 PCI DSS**

**6.2 HIPAA**

**6.3 GDPR**

**6.4 ISO 27001**

## **7. Competitor & Market Analysis**

### **7.1 Competitor Analysis**

#### **7.1.1 Comparison Table**

#### **7.1.2 What Competitors Lack**

### **7.2 Market Research**

#### **7.2.1 Market Overview**

#### **7.2.2 Zero Trust Demand**

#### **7.2.3 Market Challenges & Needs**

#### **7.2.4 Regulatory Drivers**

#### **7.2.5 Trends & Opportunities**

#### **7.2.6 Landscape Summary**

## **8. Scientific Research & Literature Review**

**8.1 Paper 1**

**8.2 Paper 2**

**8.3 Paper 3**

**8.4 Paper 4**

**8.5 Paper 5**

**8.6 Paper 6**

**8.7 Paper 7**

## **9. System Architecture**

### **9.1 High-Level Architecture Diagram**

### **9.2 Main System Components**

### **9.3 Component Communication Flow**

### **9.4 Tech Stack Summary**

## **10. Detailed Architecture of the Proxy**

**10.1 Connection Lifecycle**

**10.2 Authentication Flow**

**10.3 Query Filtering Flow**

**10.4 Policy Enforcement Flow**

**10.5 Session Monitoring Flow**

**10.6 User → Gateway → Database Diagram**

## 11. High-Level Data Flow Diagrams

### 11.1 Authentication Flow Diagram

### 11.2 Query Filtering Diagram

### 11.3 Logging & Auditing Flow Diagram

## 12. Technology Justification

12.1 Why Go

12.2 Why Node.js / TS / React

12.3 Why mTLS (and why TCP is temporary)

12.4 Why SQLite / Internal Storage

12.5 Design Decision Summary

## **13. Prototype – Semester 1**

### **13.1 Implemented Features**

### **13.2 Screenshots (CLI & Dashboard)**

### **13.3 What Works vs What Doesn't**

### **13.4 Technical Decisions Made**

### **13.5 Implementation Challenges**

## **14. Development Methodology**

### **14.1 Agile Method**

### **14.2 Meeting Structure**

### **14.3 Collaboration Tools**

### **14.4 Documentation & Observability**

## **15. Task Tracking**

**15.1 Team Task Tracking (Actual Examples)**

**15.2 Supervisor Tracking Logs**

**15.3 Blockers, Risks & Resolution Notes**

## **16. Milestones**

### **16.1 Term 1 Milestone Roadmap**

**16.1.1 Milestone 1**

**16.1.2 Milestone 2**

**16.1.3 Milestone 3**

**16.1.4 Milestone 4**

**16.1.5 Milestone 5**

### **16.2 Timeline Chart (Gantt-like)**

## **17. Threat Model & Security Considerations**

### **17.1 Threat Model**

### **17.2 Risks & Attack Vectors**

### **17.3 Mitigation Techniques**

### **17.4 Why Zero Trust is Needed**

## **18. Roadmap for Term 2**

### **18.1 Remaining Features**

### **18.2 Architecture Improvements**

### **18.3 Performance Goals**

### **18.4 Testing & Validation Plan**

## **19. Team Contribution**

### **19.1 Overview of Contribution Approach**

### **19.2 Individual Contributions**

## **20. Expected Outcomes**

## **21. Conclusion**

**21.1 Restated Purpose**

**21.2 Summary of Achievements**

**21.3 Importance & Contribution**

**21.4 Transition to Next Semester**

## **References**

## A. Glossary

## B. Dashboard Mockups