IoT (D)DoS prevention and corporate responsibility

A model to prevent internet pollution and liability claims alike

---

S. Scholtes

June 7, 2019

Research Project 2
Master of System and Network Engineering
Institute of Informatics
University of Amsterdam

Outline

- Motivation
- Growth aspects
- Legislative developments
- Related work
- Research question
- Model
- Conclusion
- Discussion
- Future work

Introduction

Motivation (D)DoS & IoT growth

(D)DoS attacks: [5] [4]

1. 620Gbps attack - 20 September 2016 on KrebsOnSecurity.com.
2. 990Gbps attack - 22 September 2016 on hosting provider OVH.
3. 1.2Tbps attack - October 2016 on DNS provider Dyn.
4. 1.3Tbps attack - February 2018 on on Github.
5. 1.7Tbps (alleged) - February 2018, victim undisclosed.

Motivation (D)DoS & IoT growth

(D)DoS attacks: [5] [4]

1. 620Gbps attack - 20 September 2016 on KrebsOnSecurity.com.
2. 990Gbps attack - 22 September 2016 on hosting provider OVH.
3. 1.2Tbps attack - October 2016 on DNS provider Dyn.
4. 1.3Tbps attack - February 2018 on on Github.
5. 1.7Tbps (alleged) - February 2018, victim undisclosed.

IoT growth: [8]

1. 2019 - 14.2 billion "things" in use.
2. 2021 - 25 billion "things" in use.
3. 76.05% growth in 2 years.

Legislative (international)

Viktor Vitowsky: [14]

1. Make IoT manufacturers liable based on section 5 from the Federal Trade Commission (FTC).
2. Businesses damaged by IoT launched DDoS attacks could bring civil claims.

Senator Mark R. Warner asked the Federal Communications Commission (FCC): [15]

1. Internet Service Provider (ISP) policing.
2. Minimum technical security standards defined by the FCC.

Legislative (national)

House of representatives asked the Ministry of Justice and Security: [9]

1. Develop a quality mark or control stamp
2. internet service providers (ISP) and telecommunication companies have enough capabilities to detect insecure IoT devices.

Research question

How can organisations prevent contributing to Internet of Things denial of service attacks?

Research question

How can organisations prevent contributing to Internet of Things denial of service attacks?

1. Detection methods

Research question

How can organisations prevent contributing to Internet of Things denial of service attacks?

1. Detection methods
2. Prevention methods

Research question

How can organisations prevent contributing to Internet of Things denial of service attacks?

1. Detection methods
2. Prevention methods
3. Minimise contribution

Related Work

- Muhammad UmarFarooq et al. and Antoine Gallais et al. list different IoT security attacks [6] [7].
- Mukrimah Nawir et al. shows the taxonomy of attacks in IoT environments [12].
- Elike Hodo et al. uses an artificial neural network to detect threats in an IoT environment [10].
- Andria Procopiou et al. developed "ForChaos" which detects denial of service attacks using forecasting and chaos theory [13].
- Daniel Jeswin Nallathambi et al. use honeypots to mitigate denial of service attacks in IoT environments [2]
- A blockchain mitigation solution is presented by Minhaj Ahmad Khan et al. [11].

Model

IoT architecture

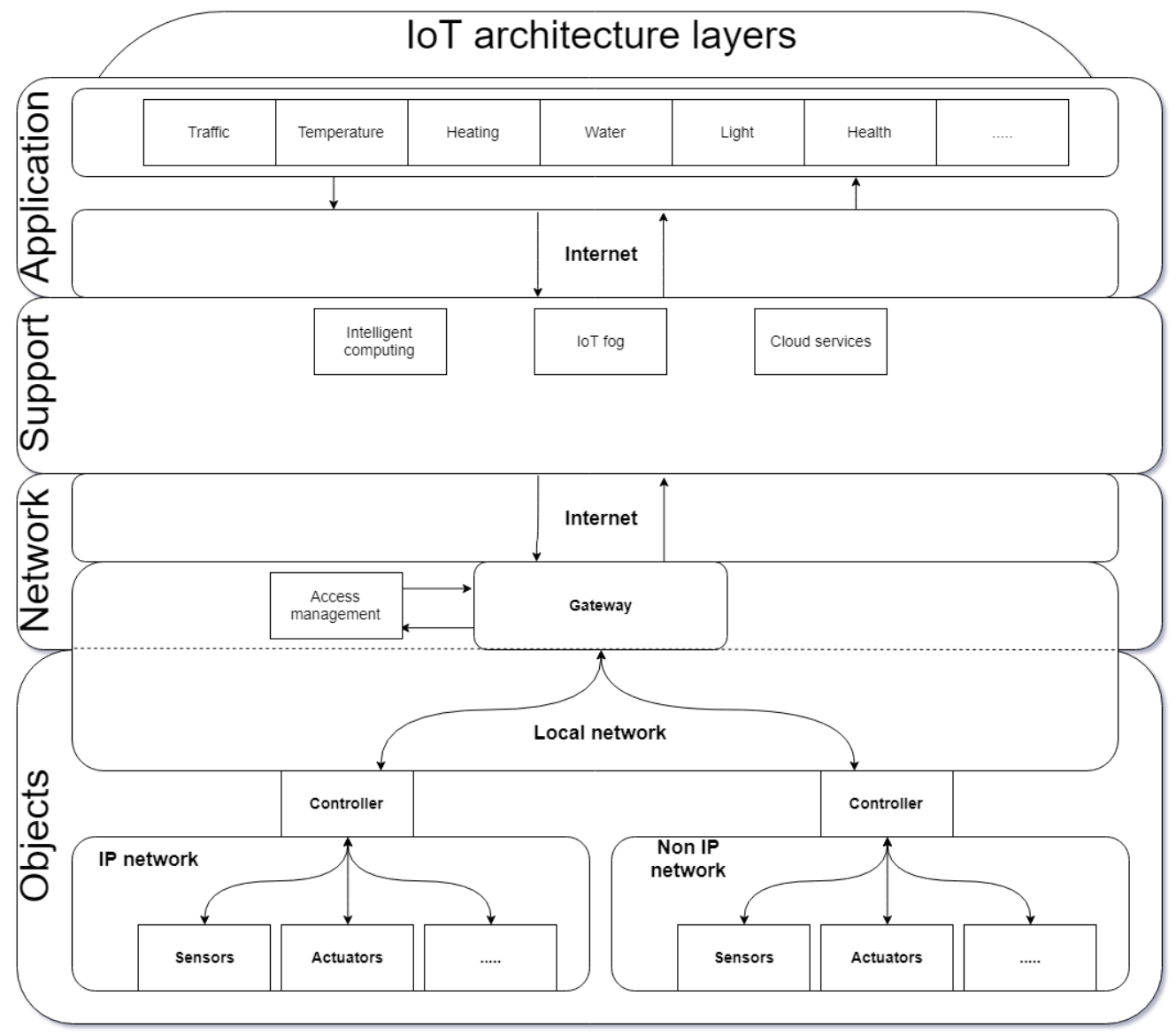

Figure 1: IoT architecture (Adapted from: [3][6][1])

IoT defensive layers

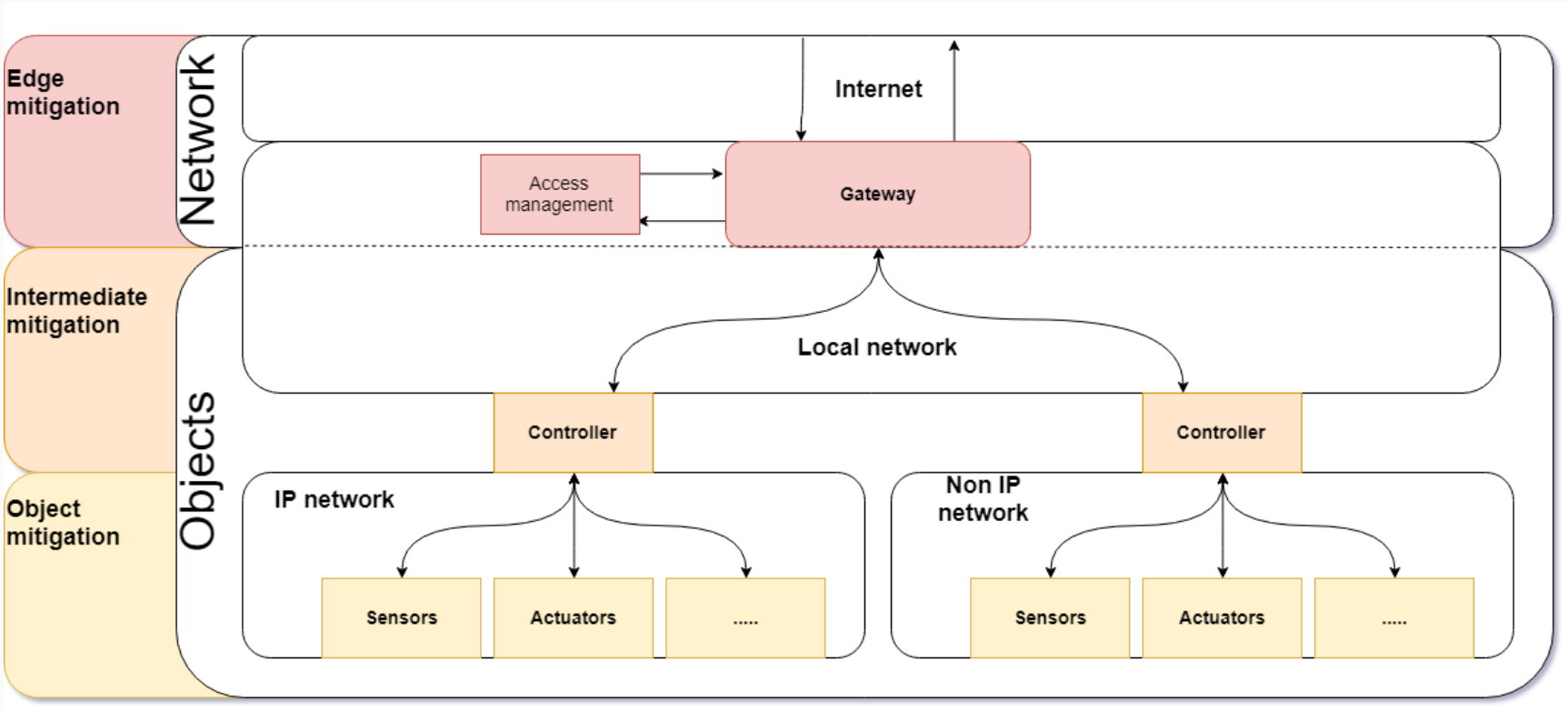

Figure 2: IoT defensive layers

Module overview

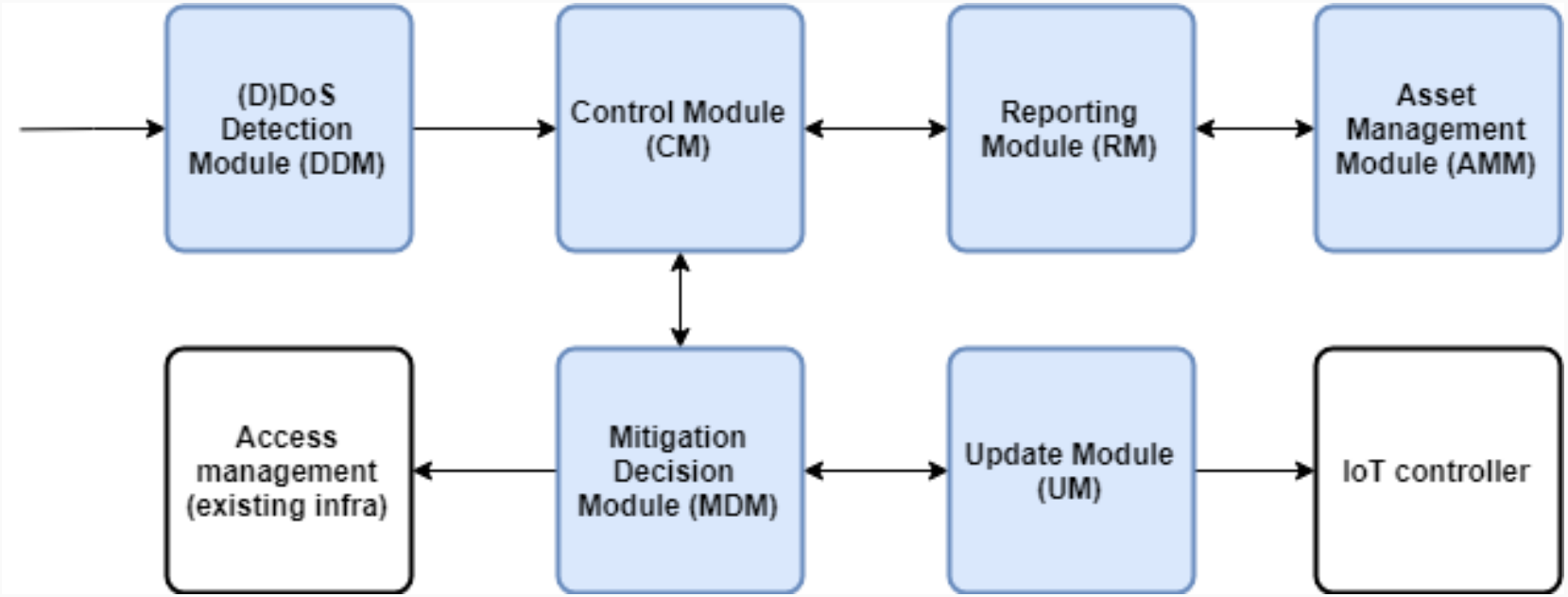

Figure 3: Module overview

(D)DoS Detection Module (DDM)

(D)DoS Detection Module (DDM) logic

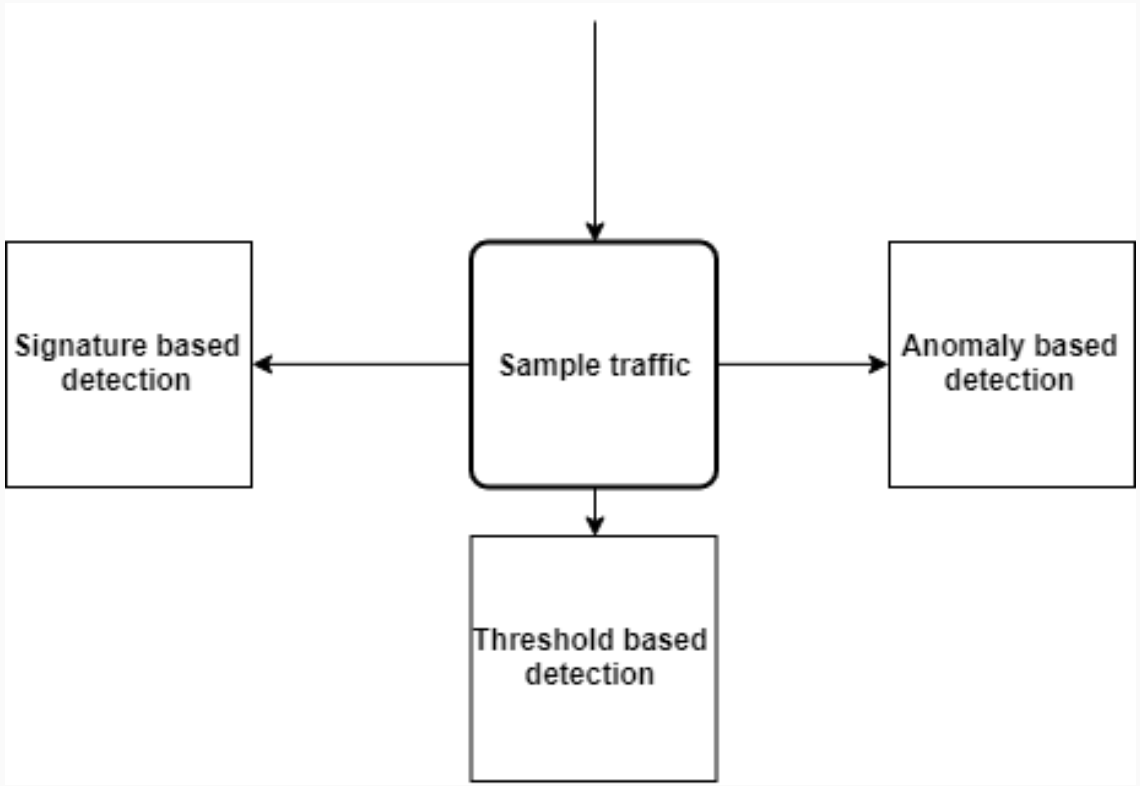

Figure 4: Detection methods

(D)DoS Detection Module (DDM) logic

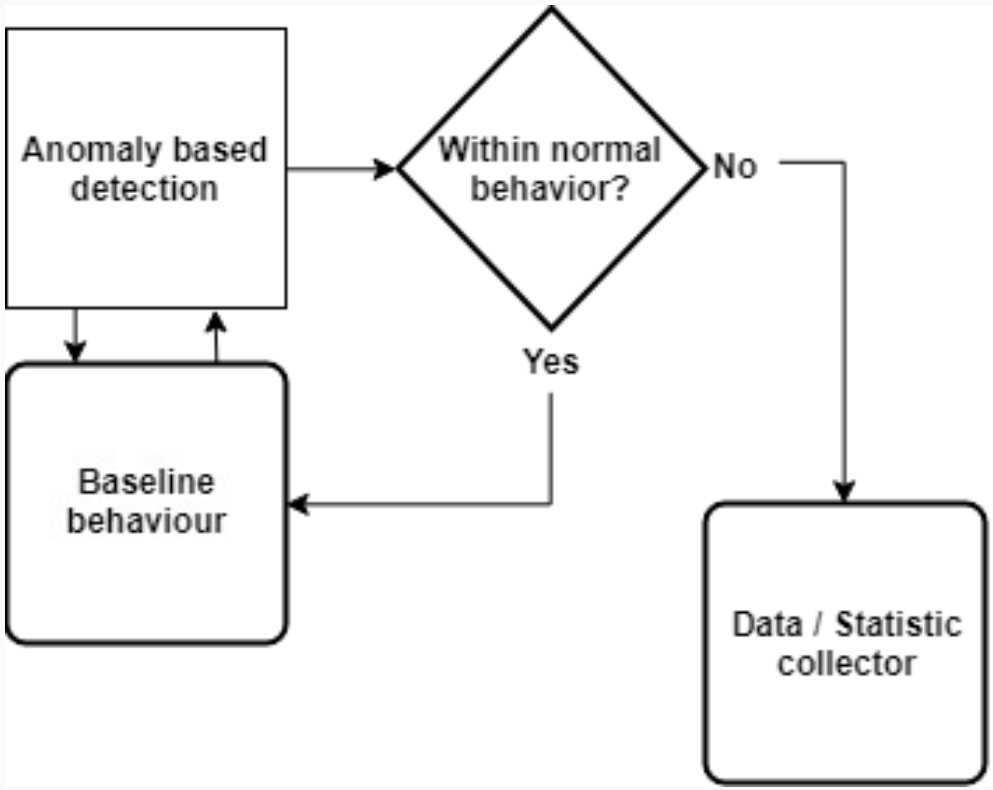

Figure 5: Anomaly logic

(D)DoS Detection Module (DDM) logic

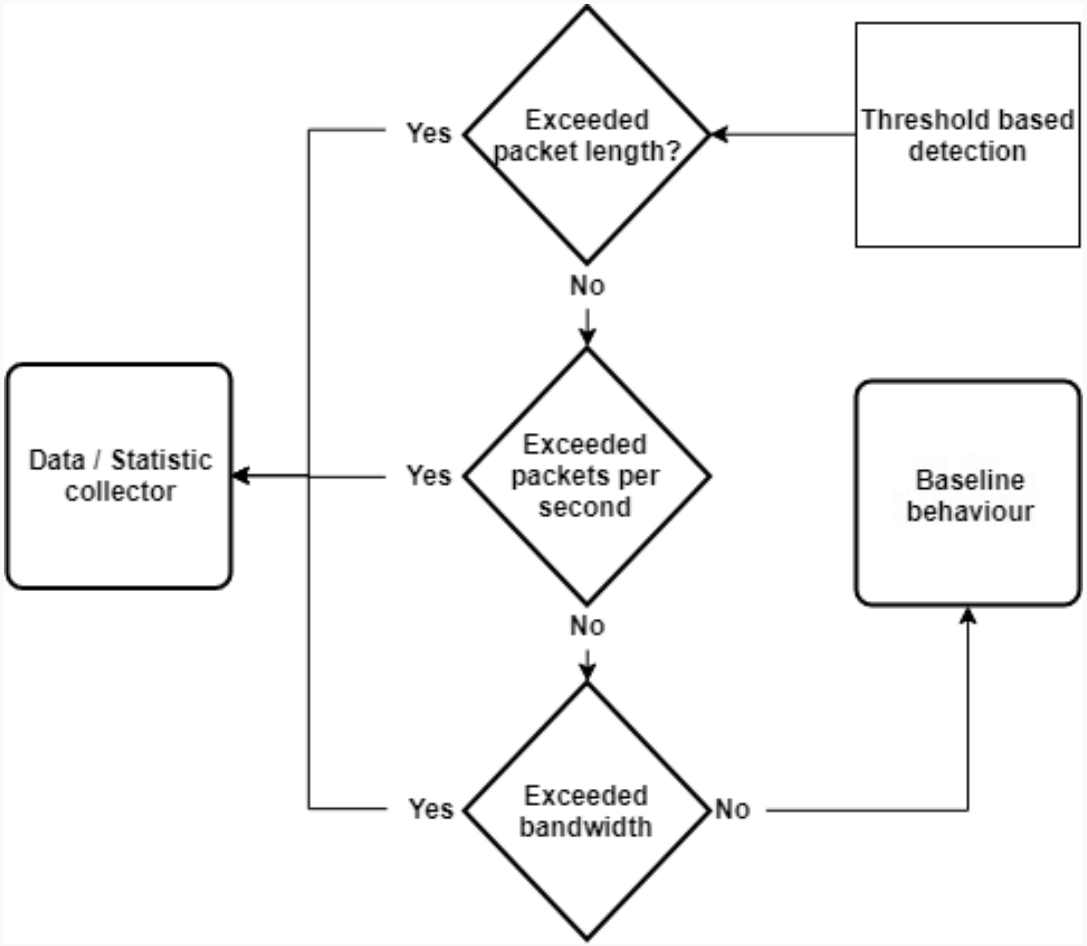

Figure 6: Threshold detection

(D)DoS Detection Module (DDM) logic

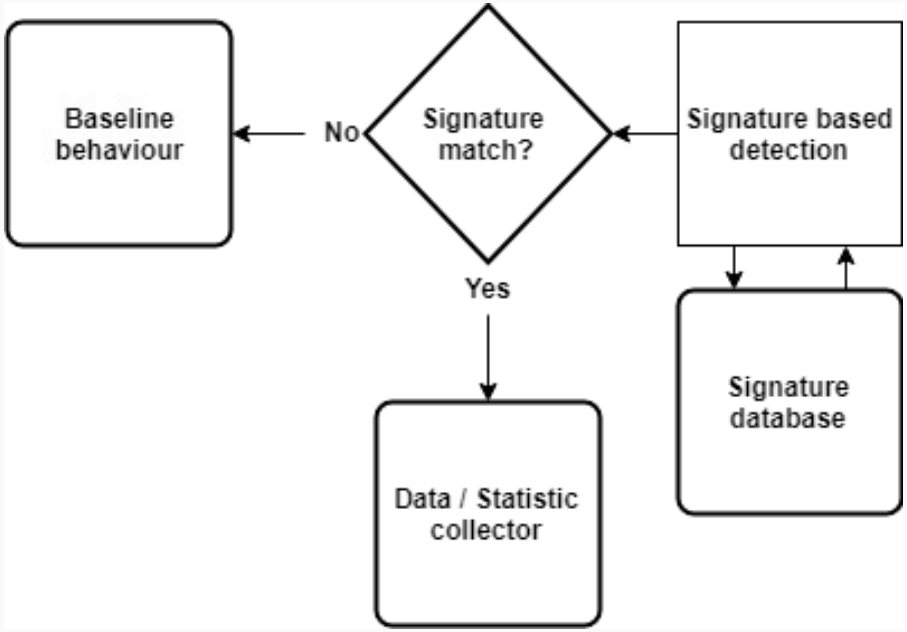

Figure 7: Signature detection

(D)DoS Detection Module (DDM) logic

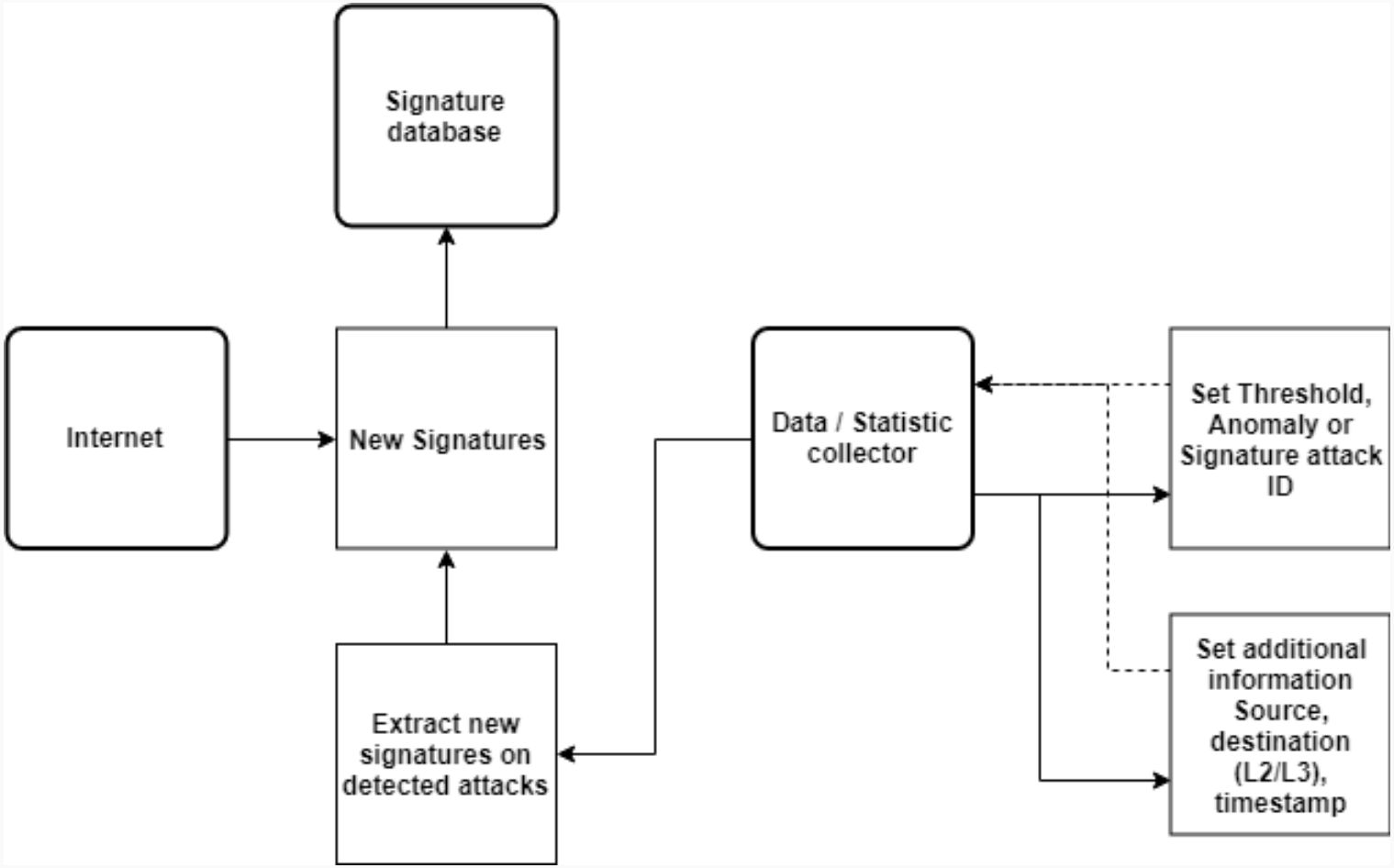

Figure 8: Statistic collector

Control Module (CM)

Control Module (CM) logic

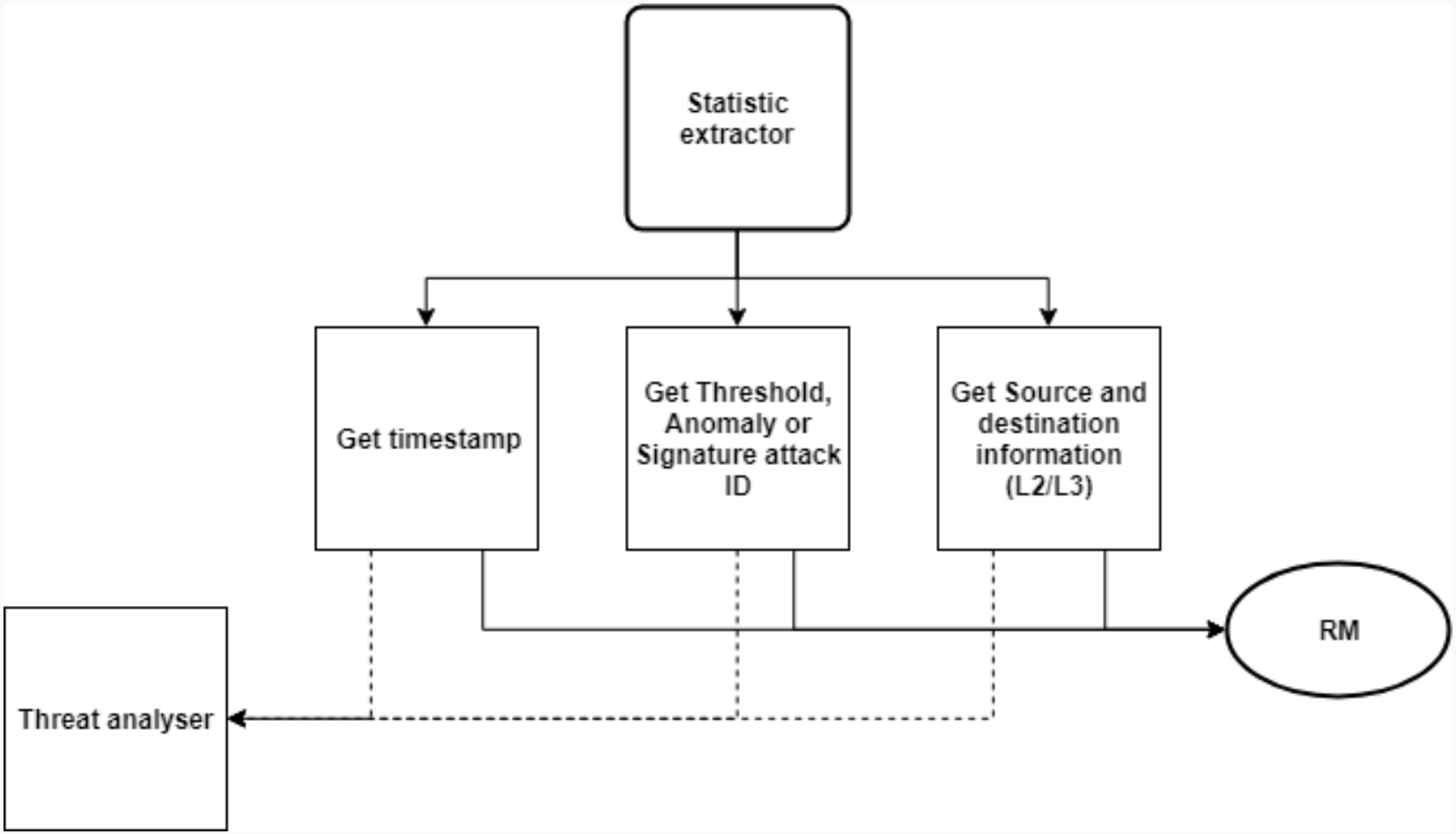

Figure 9: Statistic extractor

Control Module (CM) logic

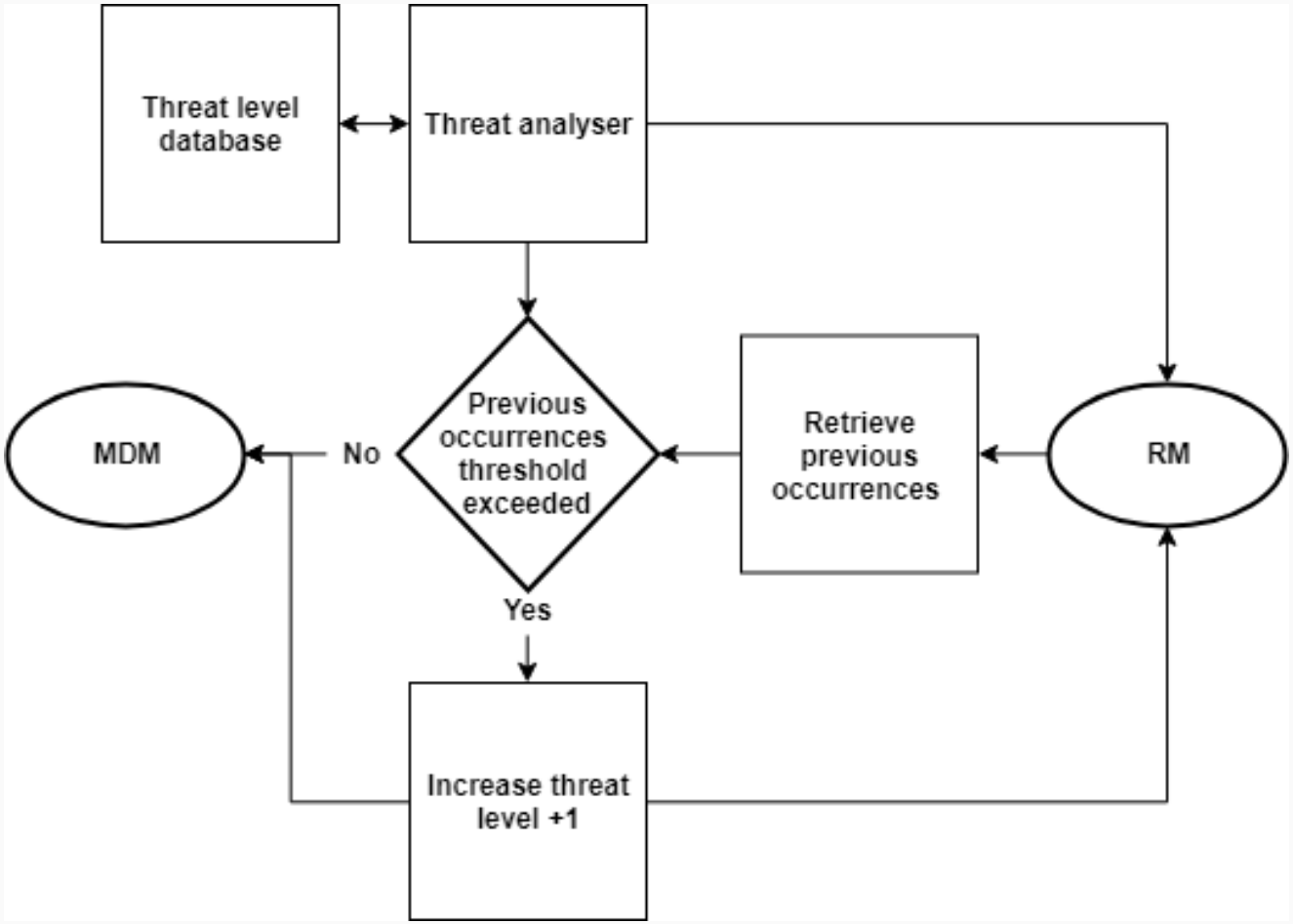

Figure 10: Threat analyser

Control Module (CM) logic

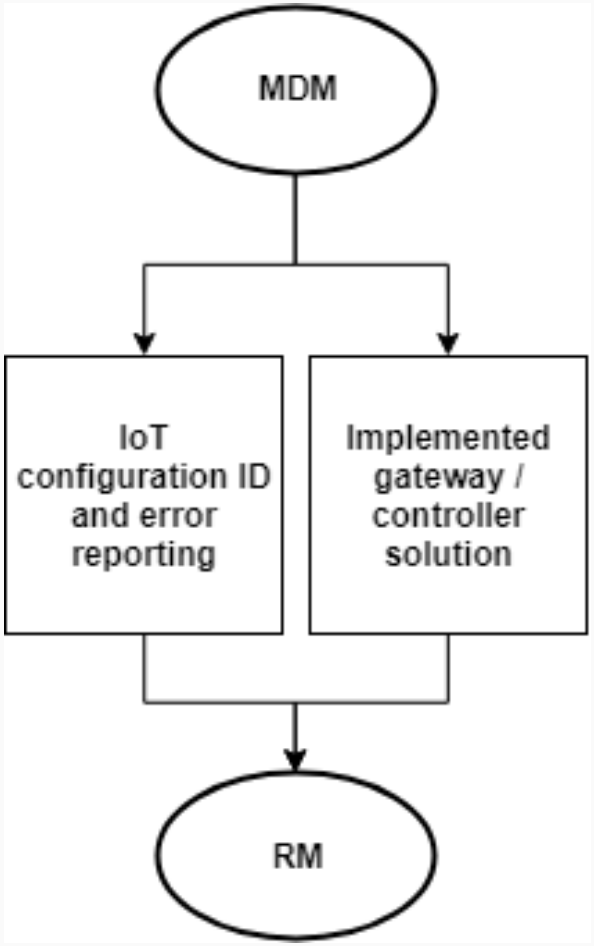

Figure 11: Lower modules information pass-through

Mitigation Decision Module (MDM)

Mitigation Decision Module (MDM) logic

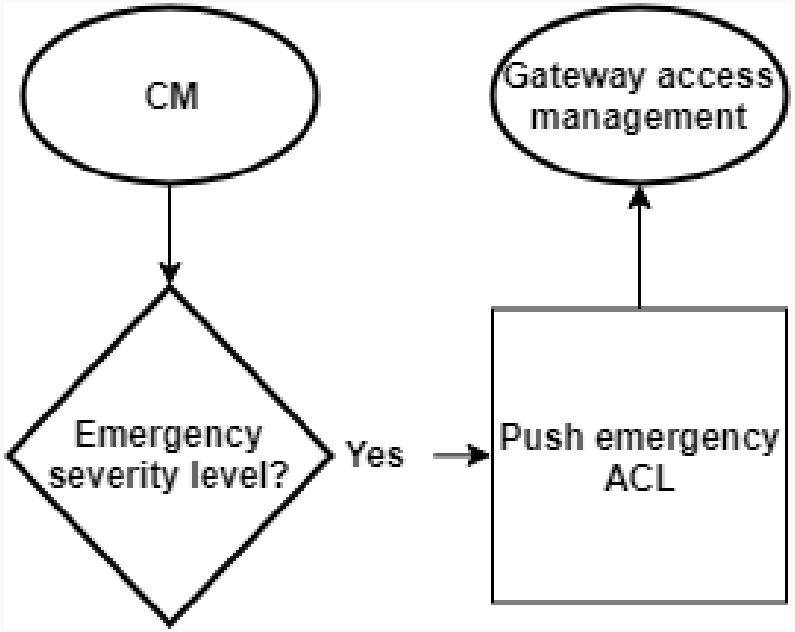

Figure 12: Emergency ACL

Mitigation Decision Module (MDM) logic

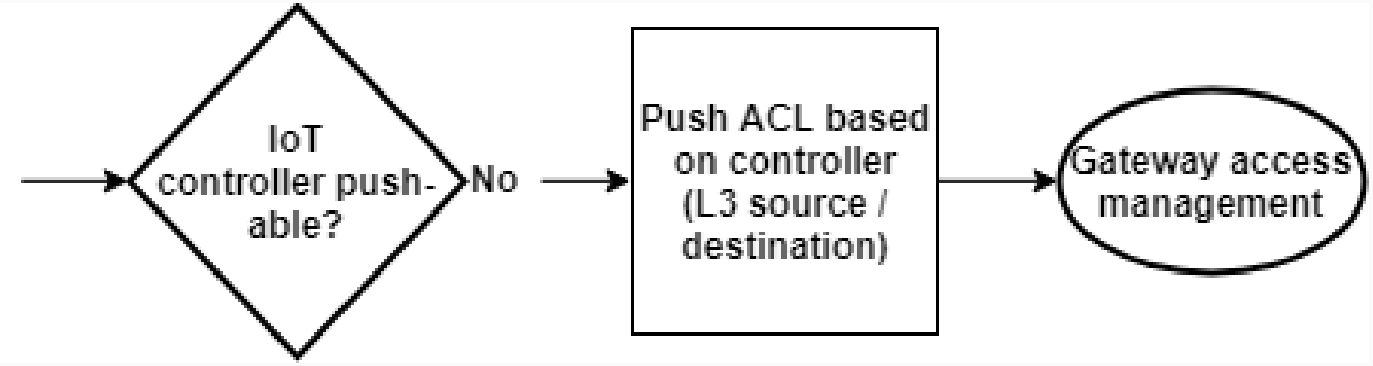

Figure 13: IoT controller update push check

Mitigation Decision Module (MDM) logic

Figure 14: IoT controller update push check

Mitigation Decision Module (MDM) logic

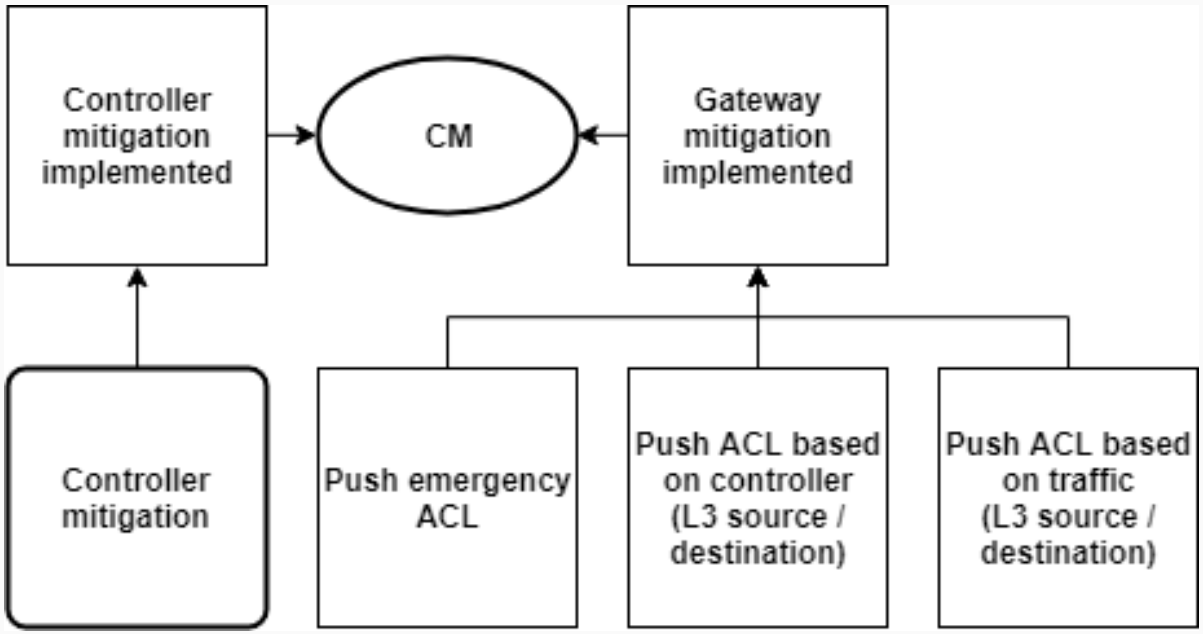

Figure 15: Reporting implemented mitigation solutions

Mitigation Decision Module (MDM) logic

Figure 16: Reporting lower module information

Update Module (UM)

UM logic

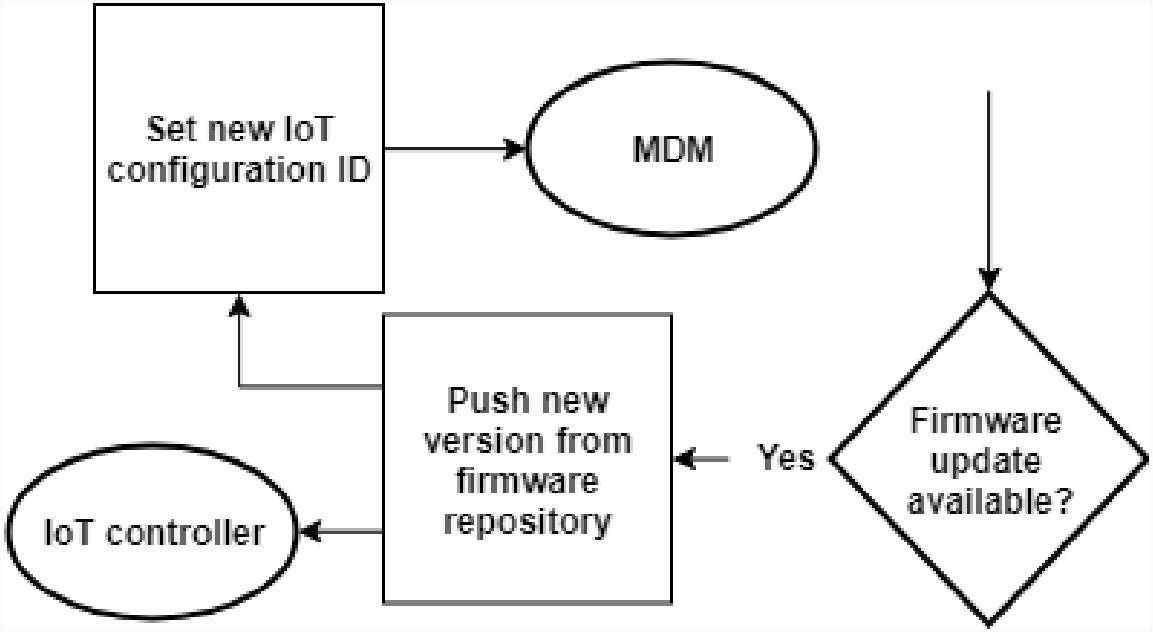

Figure 17: IoT controller firmware check

Update Module (UM) logic

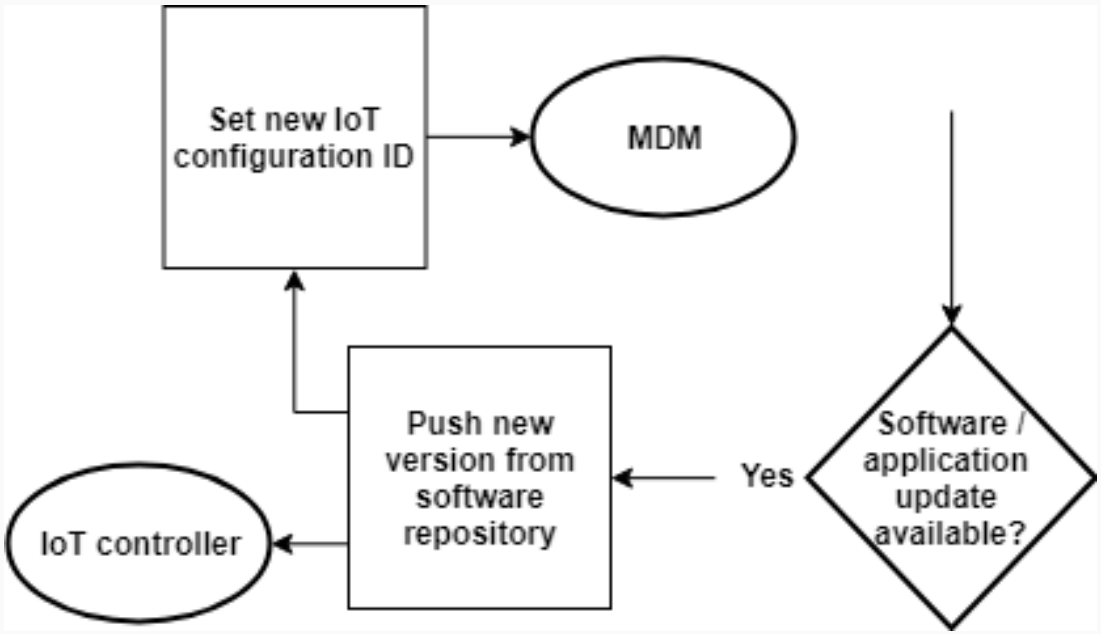

Figure 18: IoT controller software check

Update Module (UM) logic

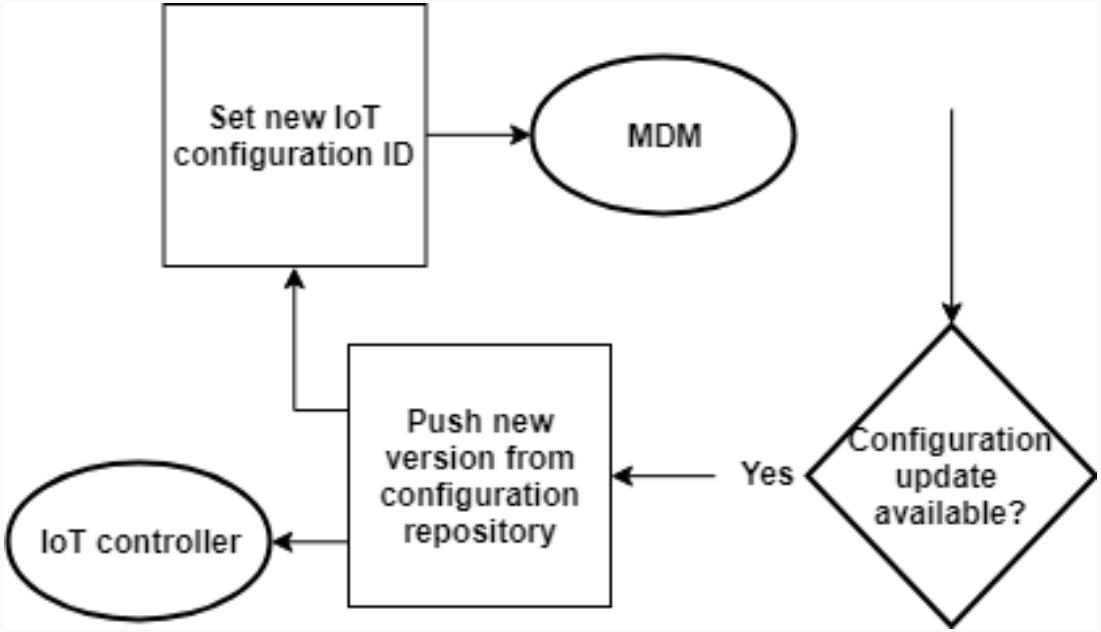

Figure 19: IoT controller configuration check

Update Module (UM) logic

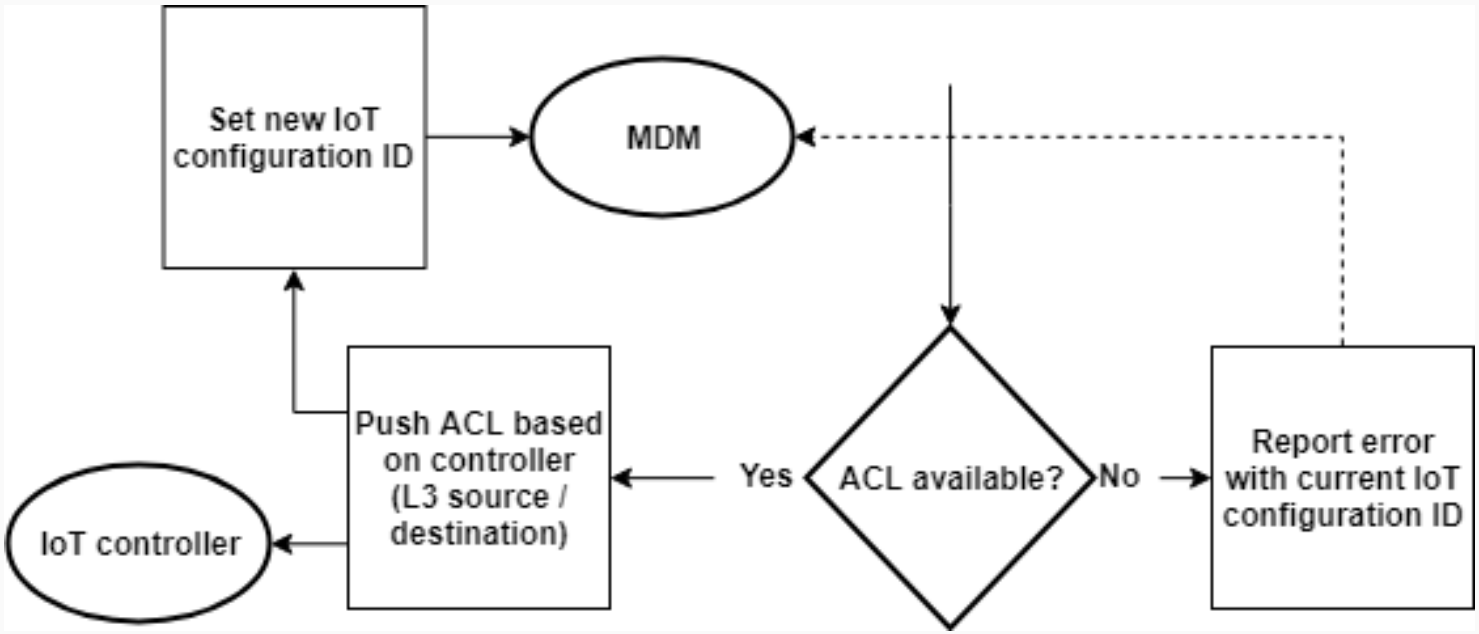

Figure 20: IoT controller access control list check

Report Module (RM)

Report Module (RM) logic

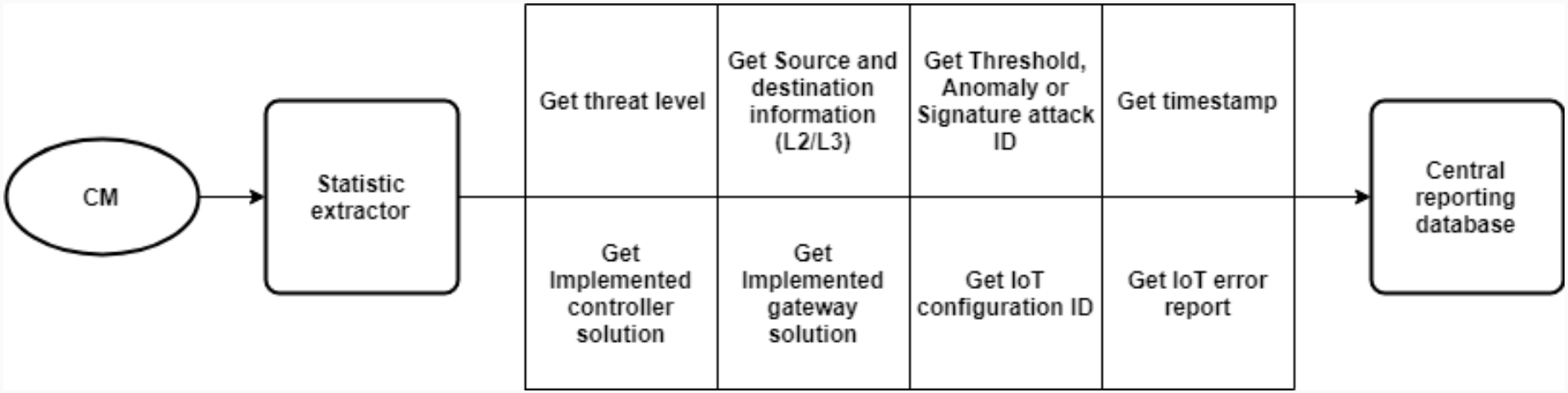

Figure 21: Statistic extractor

Report Module (RM) logic

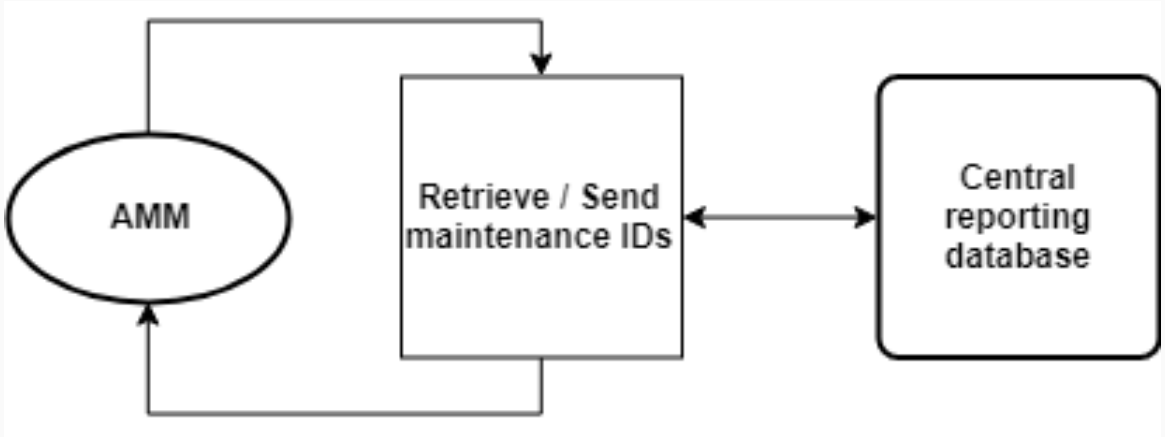

Figure 22: Maintenance ID reporting and extracting

Asset Management Module (AMM)

Asset Management Module (AMM) logic

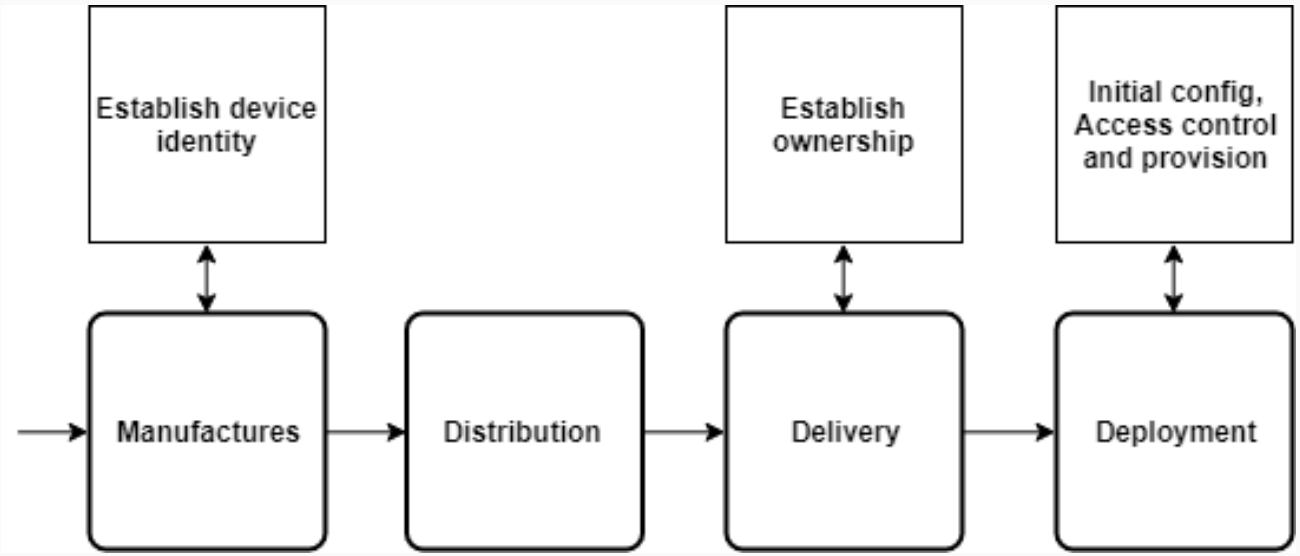

Figure 23: Manufacturers and deployment

Asset Management Module (AMM) logic

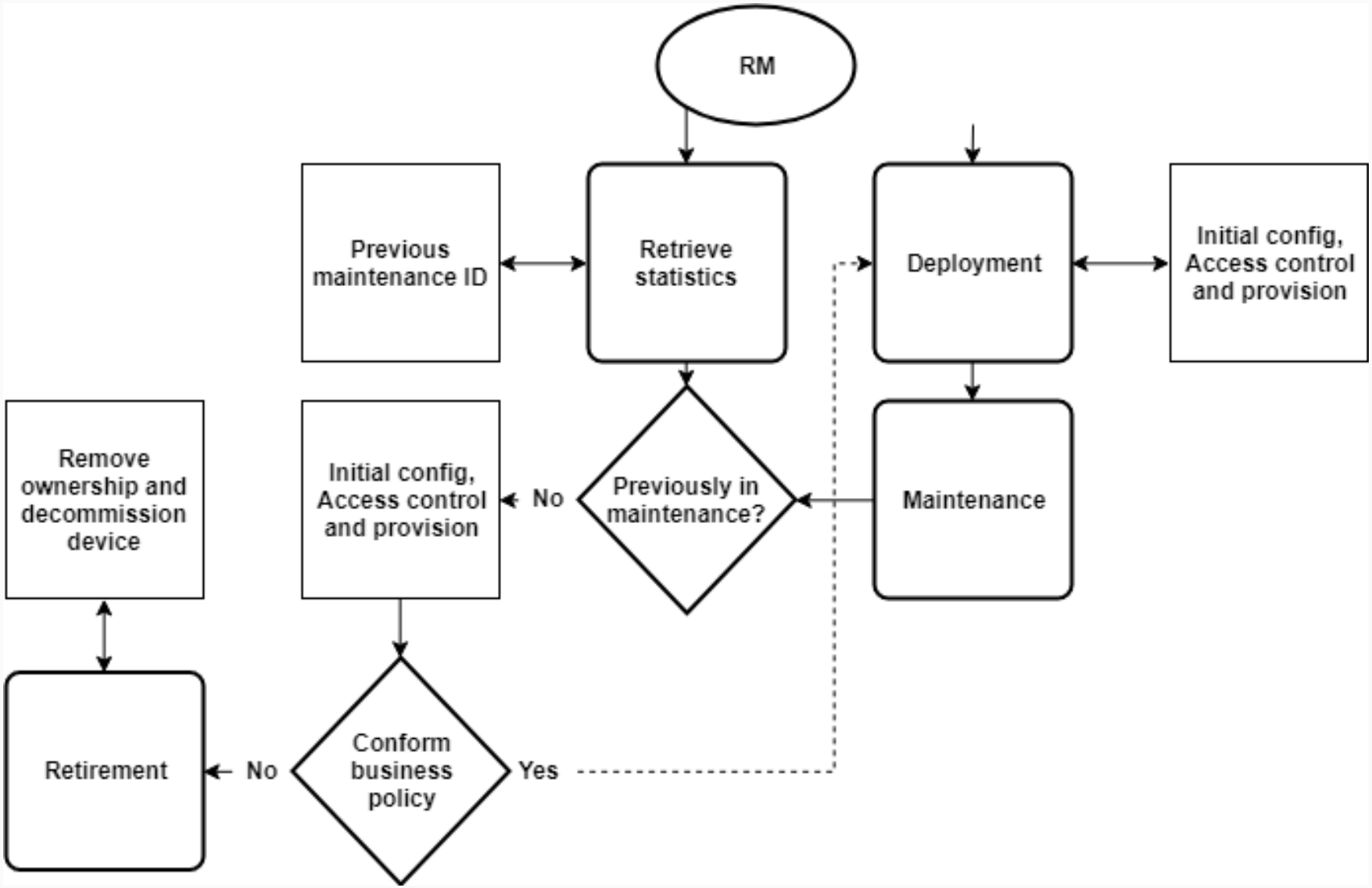

Figure 24: Previously in maintenance check

Asset Management Module (AMM) logic

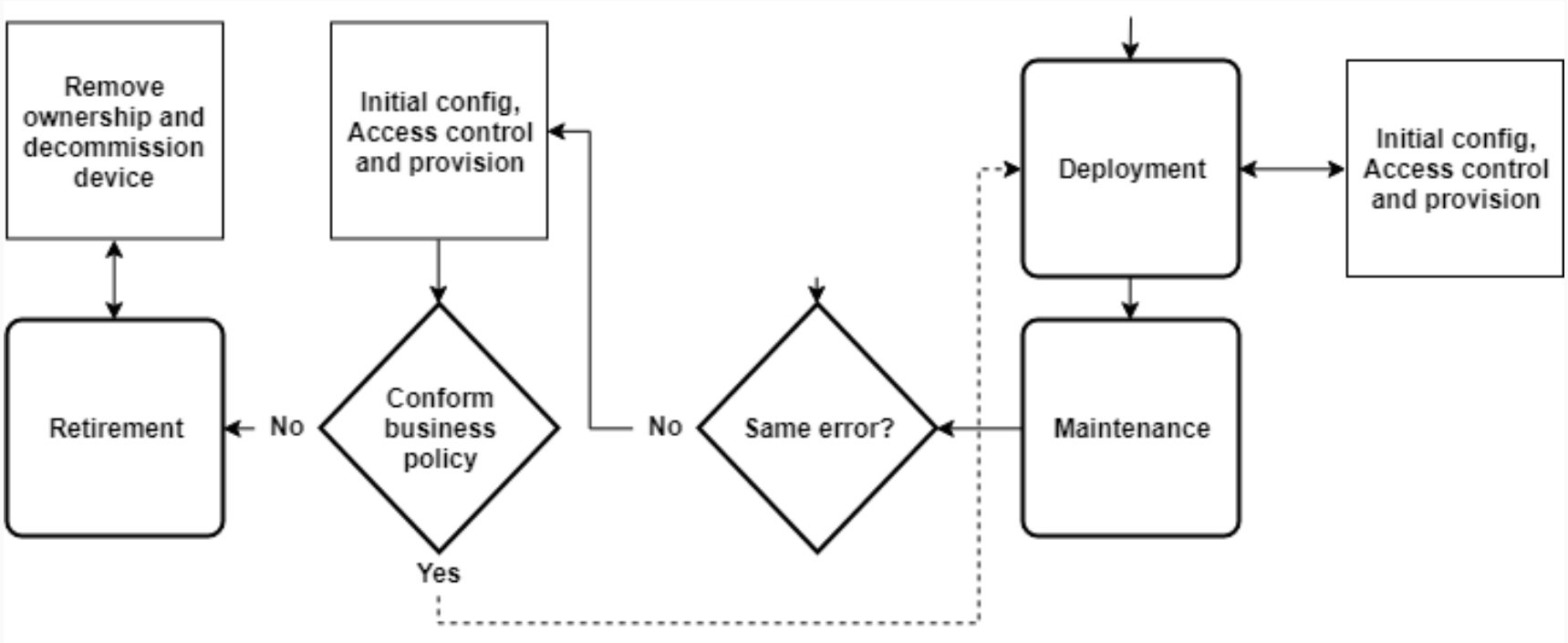

Figure 25: Same error check

Asset Management Module (AMM) logic

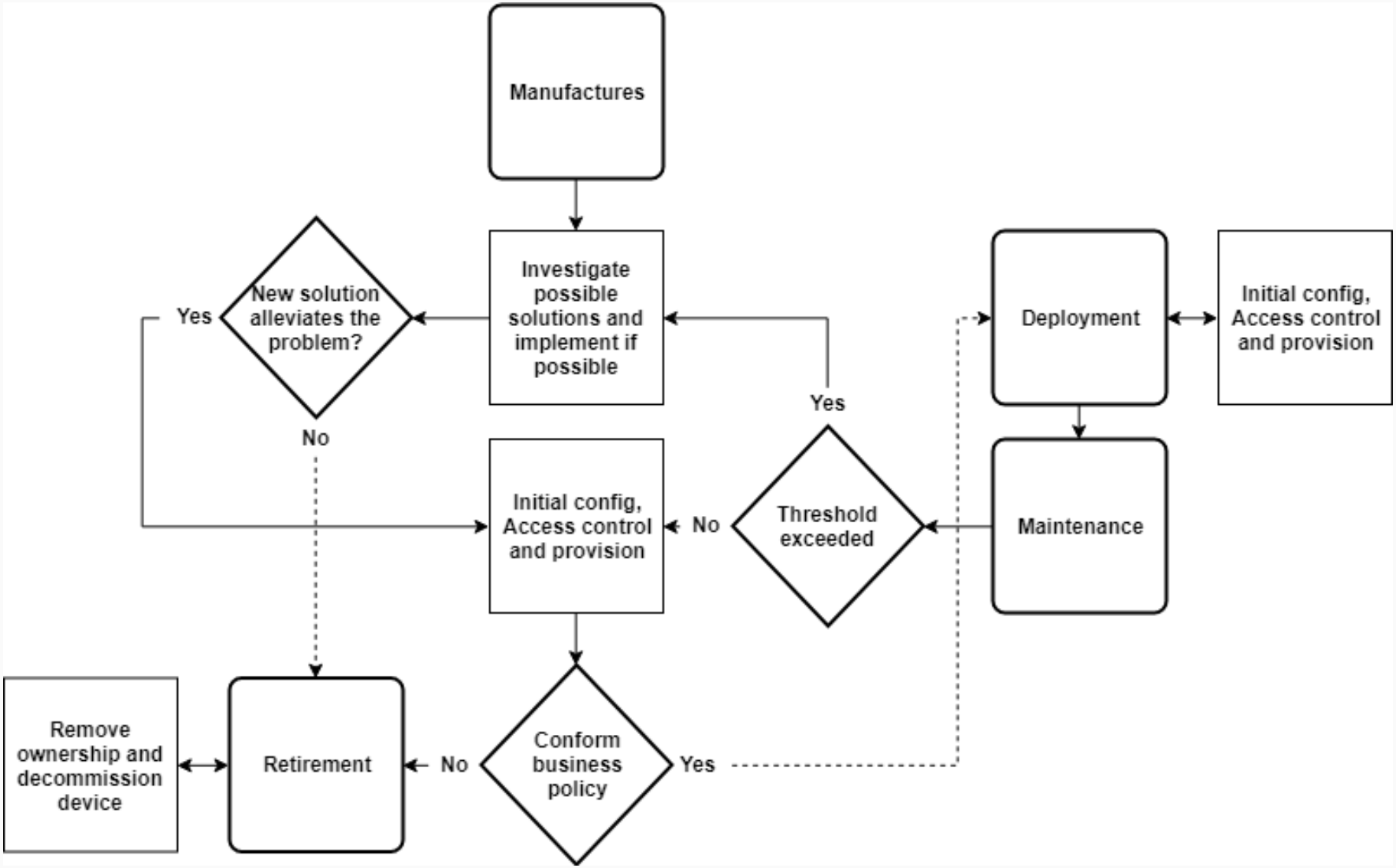

Figure 26: Error threshold check

Asset Management Module (AMM) logic

Figure 27: Error threshold check

IoT architecture with added modules

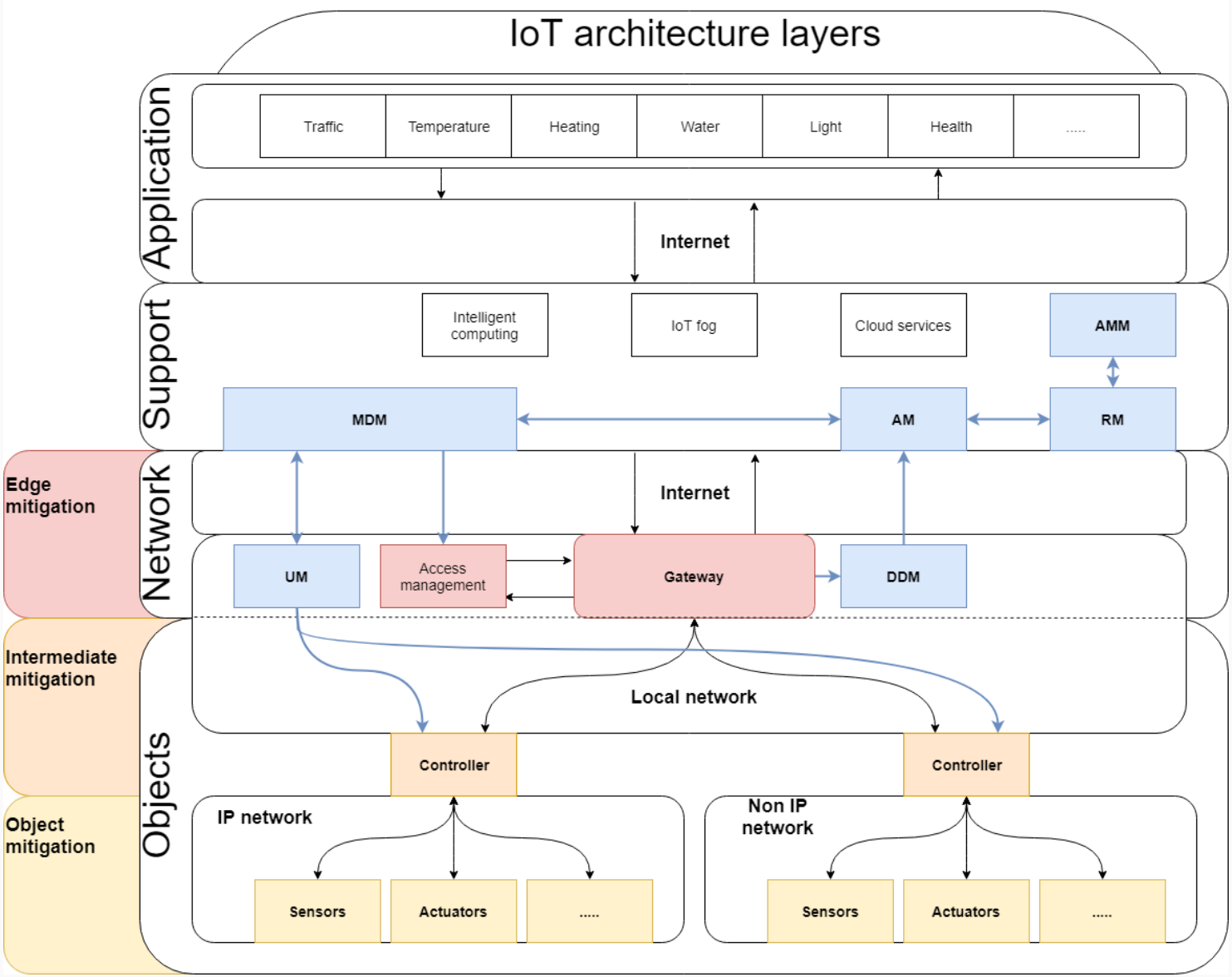

Figure 28: Modules within the IoT architecture

Conclusion, Discussion & Future Work

Conclusion

How can organisations prevent contributing to Internet of Things denial of service attacks?

Discussion

- Model applicability dependent on used IoT architecture.
- Module to device translation.
- High likely hood of availability (detection and mitigation).
- Access control list side effects.
- Layer 3 attributes.
- External influences effecting the design.

Future Work

- Proof of concept (measure performance)
  1. DDM detection methods
  2. DDM traffic sampling rate
  3. RM databases
  4. CM threat logic
- Applicable hardware setups
- Include object defensive layer
- Threat level matrix guidelines.

References i

- Vipindev Adat and BB Gupta. "Security in Internet of Things: issues, challenges, taxonomy, and architecture". In: *Telecommunication Systems* 67.3 (2018), pp. 423–441.
- M Anirudh, S Arul Thileeban, and Daniel Jeswin Nallathambi. "Use of honeypots for mitigating DoS attacks targeted on IoT networks". In: *2017 International Conference on Computer, Communication and Signal Processing (ICCCSP)*. IEEE. 2017, pp. 1–4.
- Armir Bujari et al. "Standards, security and business models: key challenges for the IoT scenario". In: *Mobile Networks and Applications* 23.1 (2018), pp. 147–154.

References ii

- Cloudflare. *Famous DDoS Attacks — The Largest DDoS Attacks Of All Time*. 2018 (accessed May 12, 2019). URL: https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/.
- enisa. *Major DDoS Attacks Involving IoT Devices*. 2016 (accessed May 11, 2019). URL: https://www.enisa.europa.eu/publications/info-notes/major-ddos-attacks-involving-iot-devices.
- Mario Frustaci et al. "Evaluating critical security issues of the IoT world: Present and Future challenges". In: *IEEE Internet of Things Journal* 5.4 (2018), pp. 2483–2495.
- Antoine Gallais et al. "Denial-of-Sleep Attacks against IoT Networks". In: *International Conference on Control, Decision and Information Technologies (CoDIT)*. 2019.

References iii

- Gartner. *Gartner Identifies Top 10 Strategic IoT Technologies and Trends*. 2018 (accessed May 13, 2019). URL: hhttps://www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends.
- *Het bericht 'Agentschap Telecom slaat alarm over hackbare apparaten'*. URL: https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2018Z10731&did=2018D32722.
- Elike Hodo et al. "Threat analysis of IoT networks using artificial neural network intrusion detection system". In: *2016 International Symposium on Networks, Computers and Communications (ISNCC)*. IEEE. 2016, pp. 1–6.

References iv

- Minhaj Ahmad Khan and Khaled Salah. "IoT security: Review, blockchain solutions, and open challenges". In: *Future Generation Computer Systems* 82 (2018), pp. 395–411.
- Mukrimah Nawir et al. "Internet of Things (IoT): Taxonomy of security attacks". In: *2016 3rd International Conference on Electronic Design (ICED)*. IEEE. 2016, pp. 321–326.
- Andria Procopiou, Nikos Komninos, and Christos Douligeris. "ForChaos: Real Time Application DDoS Detection Using Forecasting and Chaos Theory in Smart Home IoT Network". In: *Wireless Communications and Mobile Computing* 2019 (2019).
- Vincent J. Vitkowsky. "The internet of things: A new era of cyber liability and insurance". In: (2015).

References v

Mark R. Warner. *Sen. Mark Warner Probes Friday;s Crippling Cyber Attack*. 2016 (accessed May 14, 2019). URL: https://www.warner.senate.gov/public/index.cfm/pressreleases?ContentRecord_id=CD1BBB25-83E0-494D-B7E1-1C350A7CFCCA.

Questions?

Additional slides: DDM

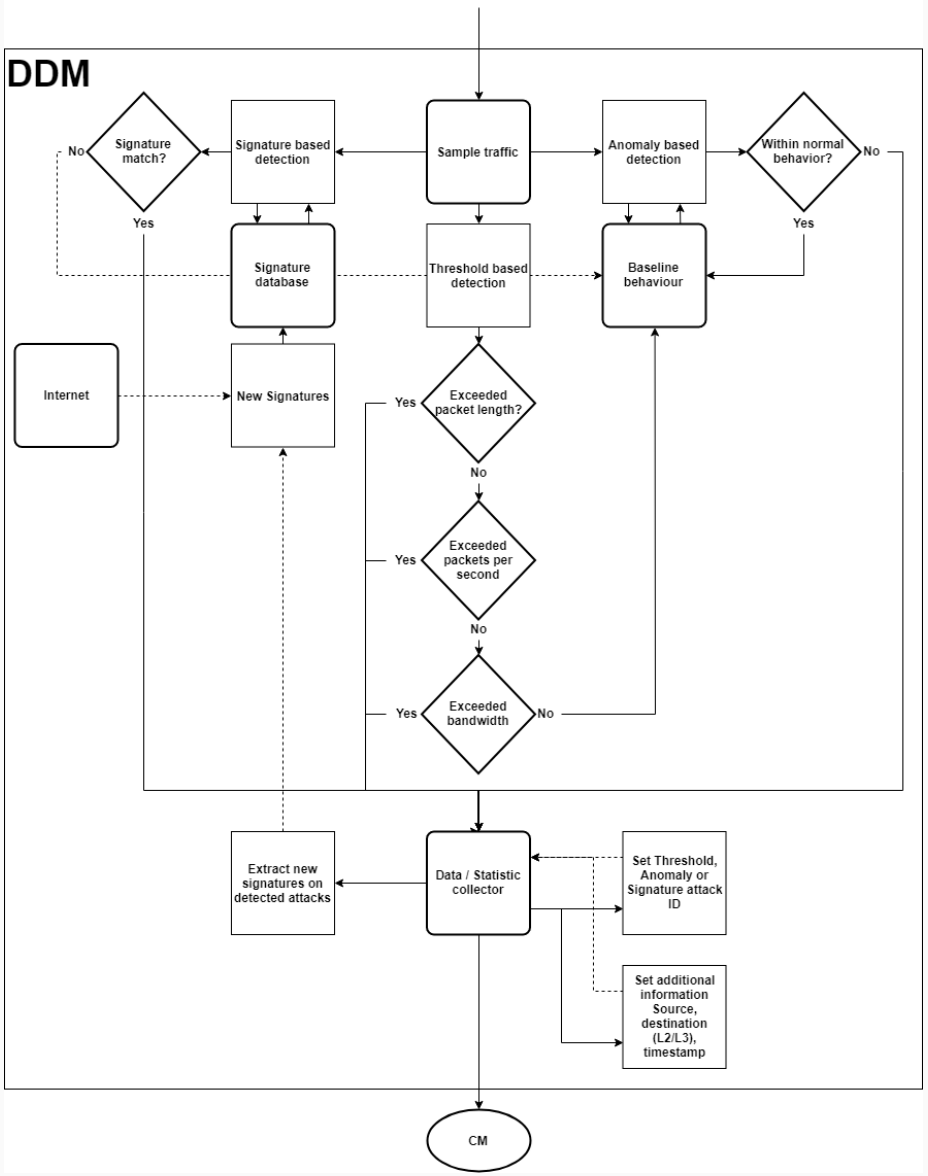

Figure 29: DDM overview

Additional slides: CM

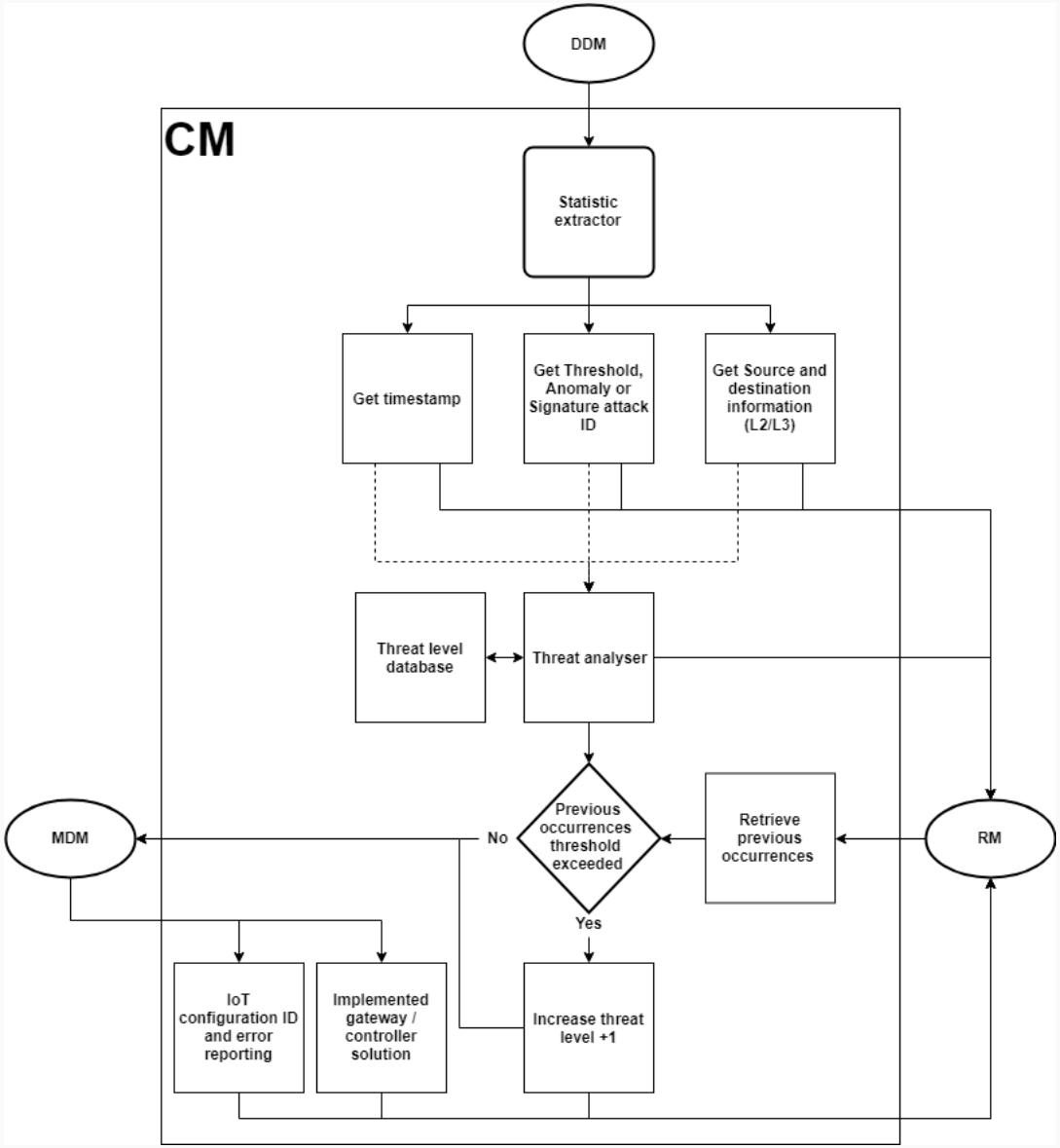

Figure 30: CM overview

Additional slides: MDM

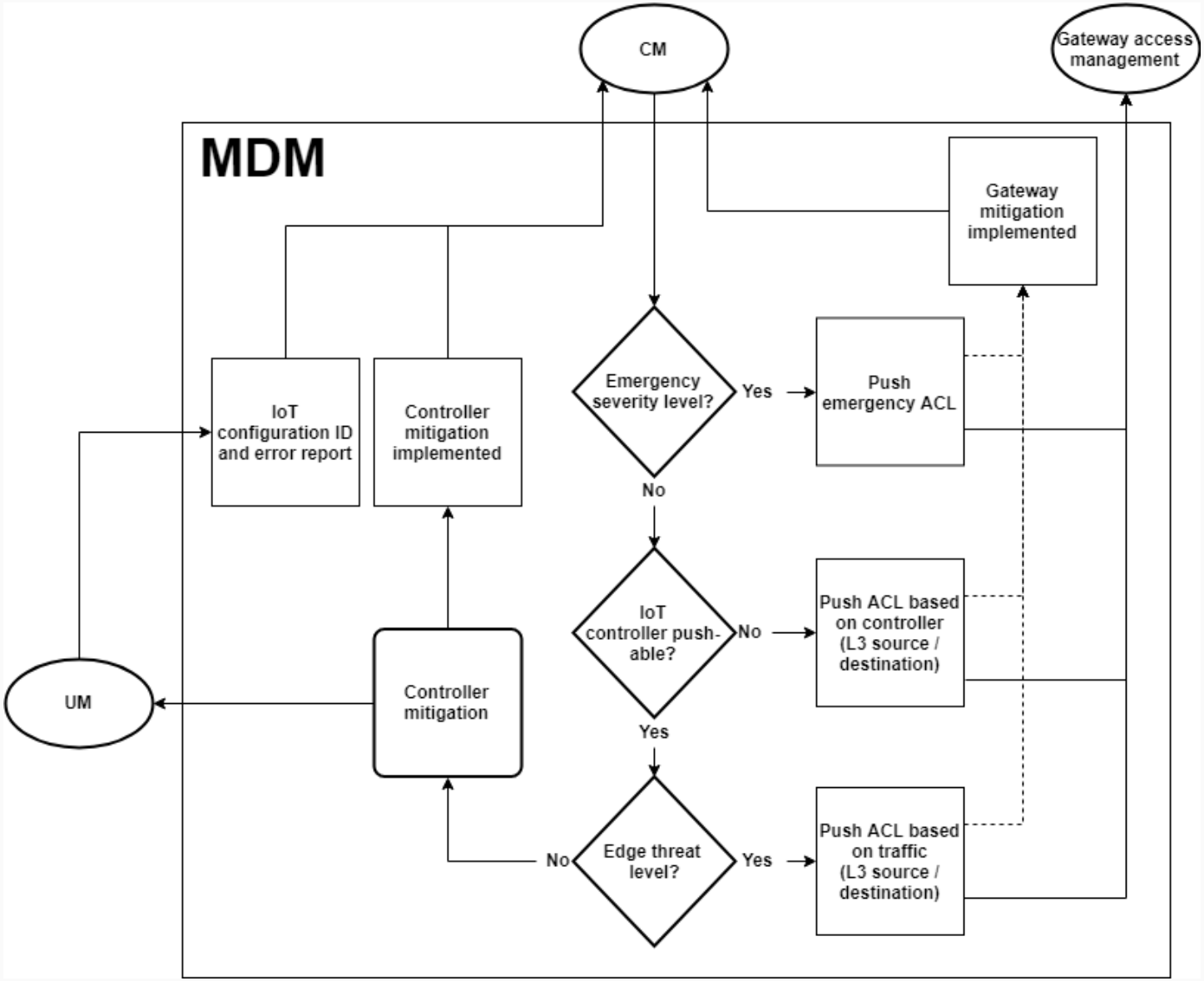

Figure 31: MDM overview

Additional slides: UM

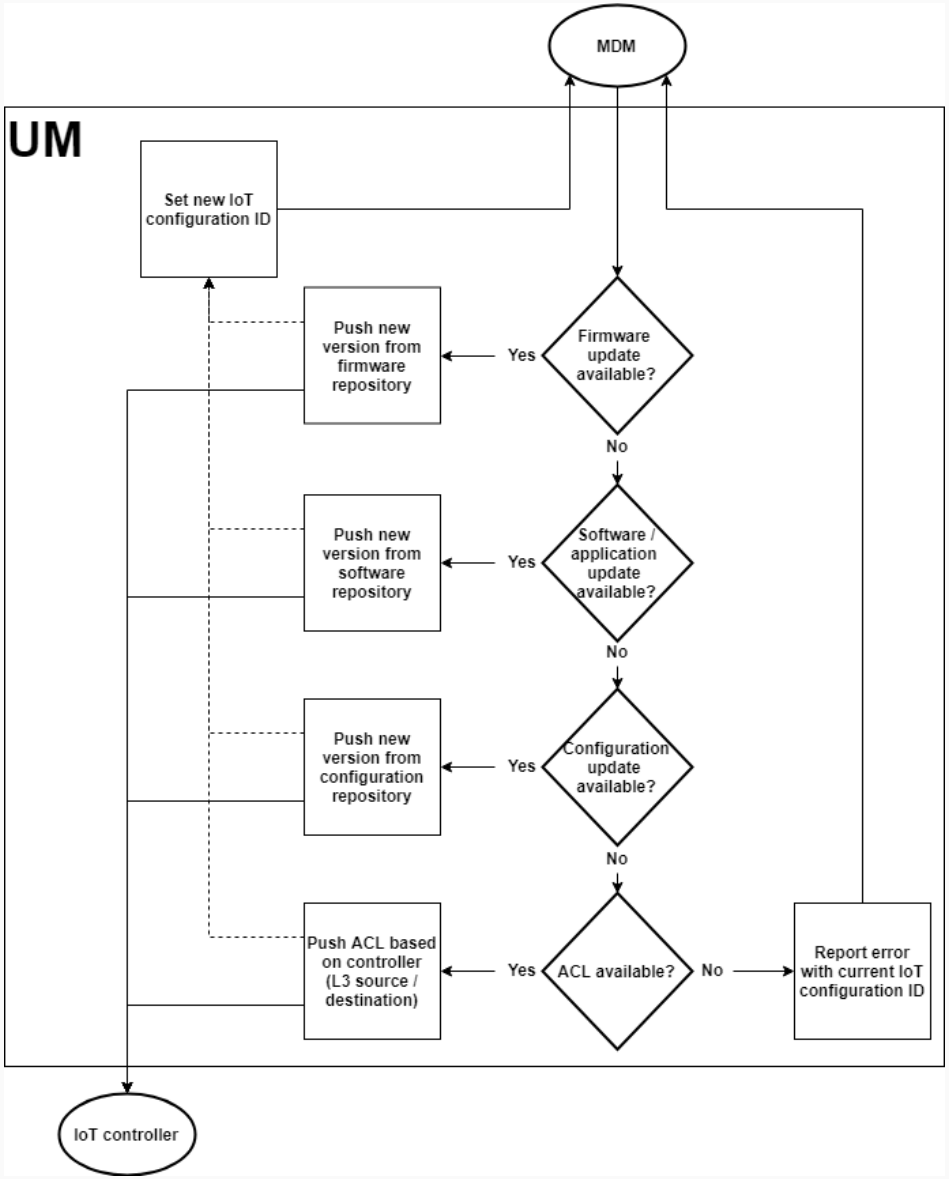

Figure 32: UM overview

Additional slides: RM

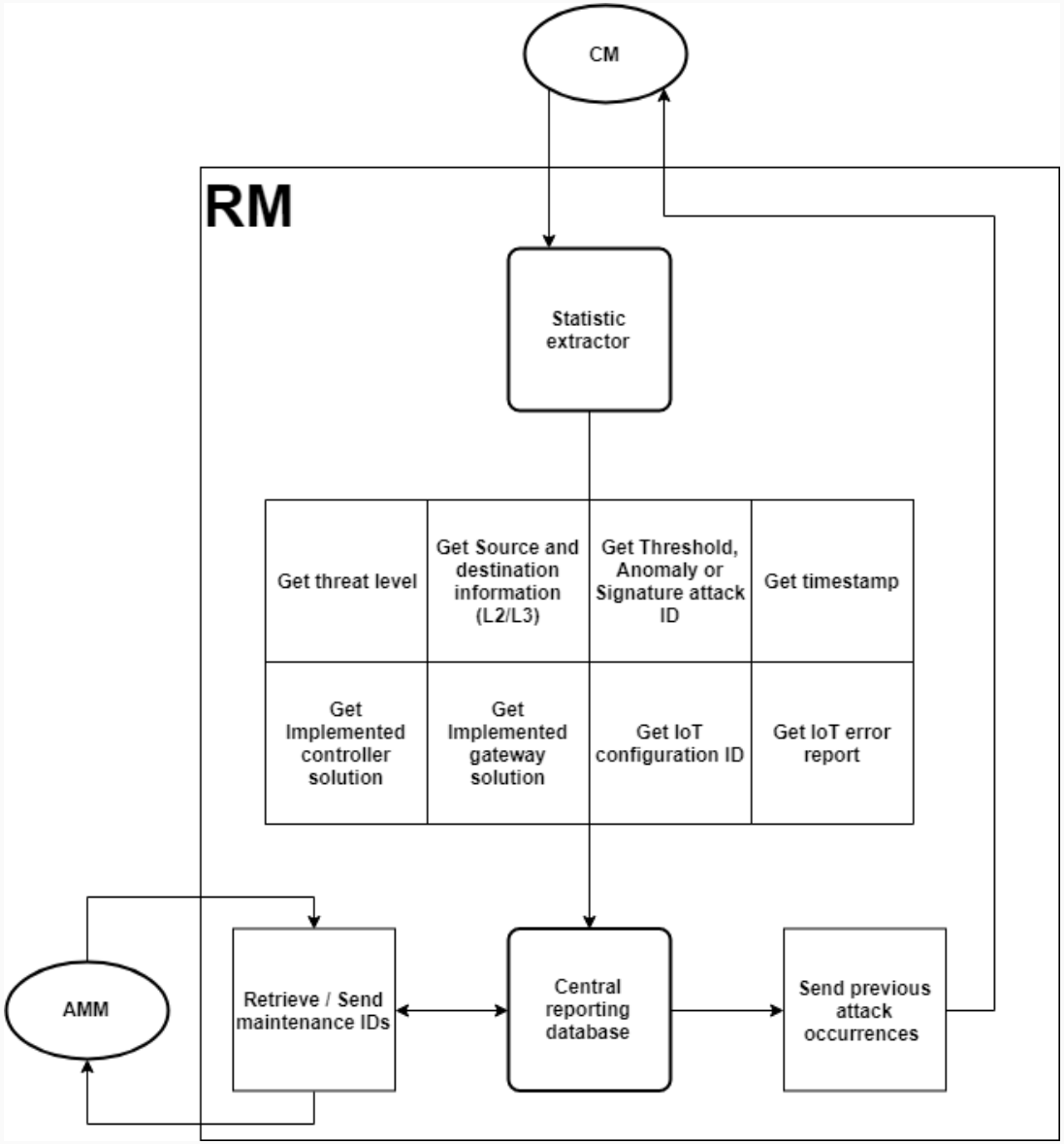

Figure 33: RM overview

Additional slides: AMM

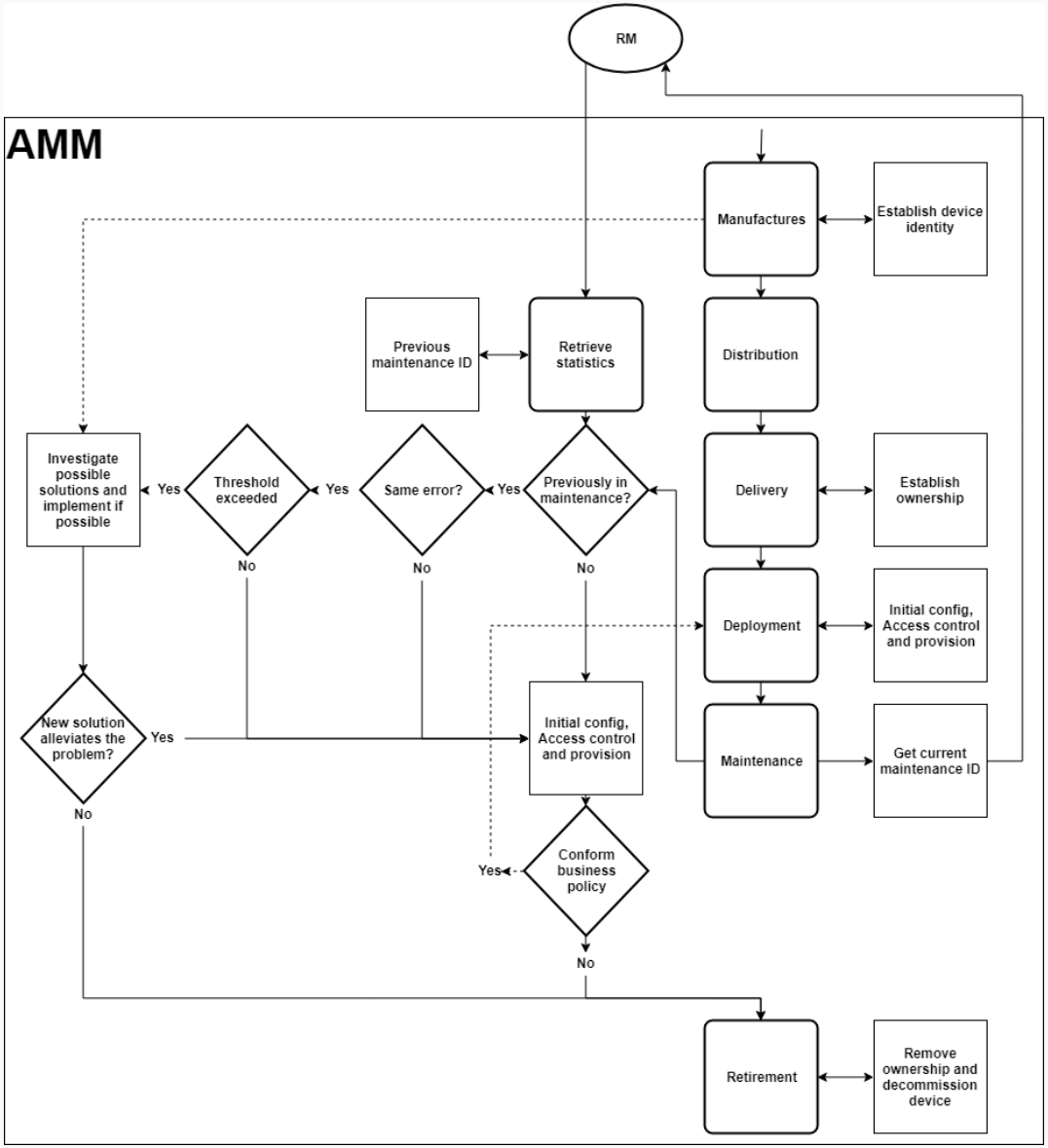

Figure 34: AMM overview