A Smart Cyber Security and Trust Management Solution for the Internet of Things (IoT)

Mohammad Dahman Alshehri
University of Technology Sydney (UTS), Centre for Artificial Intelligence (CAI)

1 Introduction

- The large number of IoT devices increases the risk of security threats such as (but not limited to) viruses or cyber-attacks.

- There is no research in ensuring that the developed IoT trust solutions are scalable across billions of IoT nodes.

- We propose a methodology for scalable trust management solution in the IoT. The methodology addresses practical and pressing issues related to IoT trust management such as trust-based IoT clustering, intelligent methods for countering bad-mouthing attacks on trust systems, issues of memory-efficient trust computation and trust-based migration of IoT nodes from one cluster to another. Experimental results demonstrate the effectiveness of the proposed approaches.

2 Motivation

- ➢ Smart clustering based approach, wherein IoT nodes are intelligent grouped into clusters based on their trust value
- ➢ Overcome memory shortage induced by extreme memory usage of node services during the storage and computation of trust computations
- ➢ Explores and develops methods to counter bad-mouthing attacks
- ➢ IoT nodes scalability

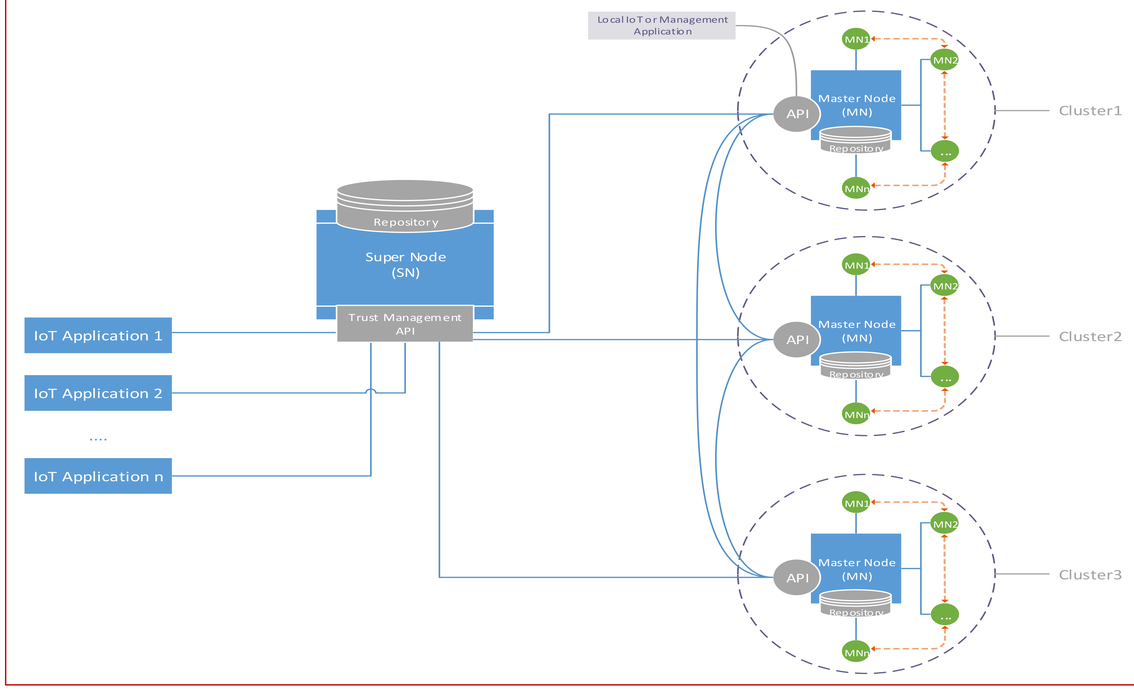
3 Challenges

- ○ Inability to scale trust solutions to billions of geographically dispersed IoT nodes
- ○ Node memory shortage for IoT nodes
- ○ Risks associated with cyber attacks on IoT

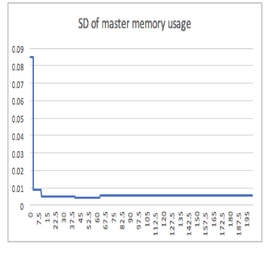
4 Smart Solution

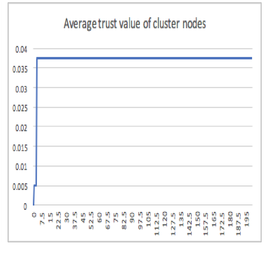
- **Algorithm 1**: A smart novel mechanism of calculating trust value for each cluster in (IoT-TM) based on memory boundaries.
- **Algorithm 2**: The conditions of nodes moving into a specified new master node in IoT-TM.
- **Algorithm 3**: Solution for extreme badmouthing attacks in IoT-TM.
- **Algorithm 4**: Smart methods for IoT nodes scalability in the platform.

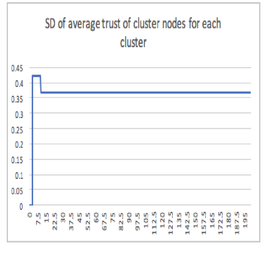
5 The Scalable Approach for Trust Management in IoT (IoT-TM)



6 Results for the Proposed Base Cases IoT-TM

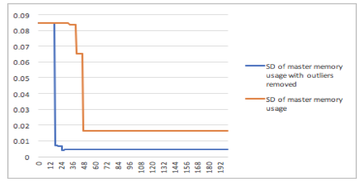


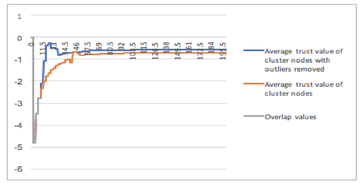


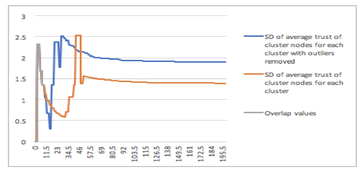


Parameter	Value
Number of nodes	343
Number of clusters	9
Simulation time	200s
Master/Cluster node memory	32 bytes
Memory rate	0.5
Trigger Outliers	True
Trigger Bad-Mouths	False
Trigger Memory Thresholds	True
Trigger Balanced Node Distribution	False

7 Results of IoT-TM Bad-Mouthing Attacks

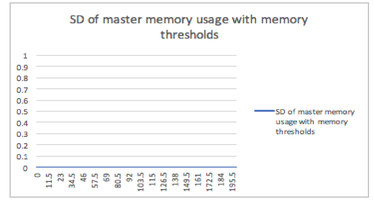


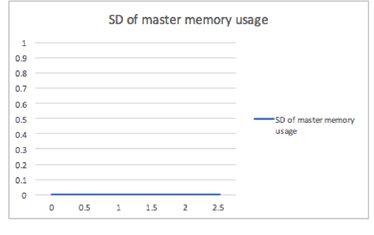




Parameter	Value
Number of nodes	343
Number of clusters	9
Simulation time	200s
Master/Cluster node memory	32 bytes
Memory rate	0.5
Trigger Outliers	Switched
Trigger Bad-Mouths	True
Trigger Memory Thresholds	True
Trigger Balanced Node Distribution	False

8 Results of Countering Extreme Memory





Parameter	Value
Number of nodes	343
Number of clusters	9
Simulation time	200s
Master/Cluster node memory	32 bytes
Memory rate	0.9775
Trigger Outliers	True
Trigger Bad-Mouths	False
Trigger Memory Thresholds	Switched
Trigger Balanced Node Distribution	True

9 Research Achievements

- ✓ **Smart solution for enabling IoT trusted platforms**
- ✓ **Recognizes badmouthing attacks and protects IoT platforms**
- ✓ **More effective memory storage for IoT nodes**
- ✓ **IoT scalability ensured**