ISO/IEC JTC 1 SC 42 Artificial Intelligence – Working Group 4

1. General

<table>
<tr><td>ID</td><td colspan="2">(leave blank, for internal use)</td></tr>
<tr><td>Use case name</td><td colspan="2">AI (Swarm Intelligence) solution for Attack Detection in IoT Environment</td></tr>
<tr><td>Application domain</td><td colspan="2">Security</td></tr>
<tr><td>Deployment model</td><td colspan="2">Hybrid or other (Agent Based Hub-Spoke)</td></tr>
<tr><td>Status</td><td colspan="2">Prototype</td></tr>
<tr><td>Scope[1]</td><td colspan="2">Anomaly Based Attack Detection in IoT environment using Swarm Intelligence</td></tr>
<tr><td>Objective(s)[2]</td><td colspan="2">Given: AMI (Advanced Metering Infrastructure – Smart Meters in Smart Buildings in Smart Cities.

Detect: Detect energy theft / meter tampering by consumer in AMI (Advanced Metering Infrastructure) or hacking attack by an external agent (man in the middle) for edge computing security scenarios with intermitted disconnection, near real-time response without using server or cloud-based analytics.</td></tr>
<tr><td rowspan="2">Narrative</td><td>Short description (not more than 150 words)</td><td>This is a unique approach to detect attacks in IoT environment using Anomaly Based Attack Detection using Swarm Intelligence methods. This is a key solution to detect energy theft scenario in Smart Metering. Energy Theft problem varies from 2% in developed countries to 35% in developing countries. This is complimentary to traditional AI or other static rule-based analysis which is heavily dependent on analysis of huge amounts of data on centralized cloud infrastructure. This solution is simple, nimble and can be run on low powered edge (IoT Nodes) for near real-time, low latency, low power, small compute, small storage Mist / Edge Computing Scenarios.</td></tr>
<tr><td>Complete description</td><td>Introduction to Anomaly Based Attack Detection using Swarm Intelligence

Motivation
▪ World-wide statistics shows there will be IoT install based of 12.86 billion units in the consumer segment by 2020.
▪ In Smart city industry, smart security is expected to account for 13.5 percent of global smart city market. There will be more than 1 billion devices installed in smart homes.</td></tr>
</table>

[1] The scope defines the intended area of applicability, limits, and audience.
[2] The intention of the system; what is to be accomplished?; who/what will benefit?.

		▪ India is planning 100 Smart cities to be developed in next 5 years, and security is of paramount importance. Securing Advanced metering Infrastructure (AMI) will be key component for securing smart city infrastructure. ▪ Important aspect of securing AMI is securing the Smart Energy meters and detecting attacks on these smart meters. ▪ While there are many traditional solutions for anomaly and intrusion-based detection based on static preset rules / policies, these solutions are not effective in detecting future attacks that are already not known. A more robust and more secure security solution to detect attacks in edge network is essential. Hence a new innovative approach of using Swarm Intelligence along with Anomaly based Detection has been a technology choice to solve this problem in a unique way. **Problem Statement** Detect energy theft / meter tampering by consumer in AMI (Advanced Metering Infrastructure) or hacking attack by an external agent (man in the middle) for edge computing security scenarios with intermitted disconnection, near real-time response without using server or cloud-based analytics. **Current situation** There are many cloud based centralized solutions available using static rules / policies configured which can detect existing known attack only. Processing in centralized cloud involves transferring data from sensors / actuator to cloud which in itself is a concern in terms of privacy, security, regulations & compliance for some key industry verticals. **Solution Approach** Swarm Intelligence is a specific branch of AI. A new innovative approach using swarm intelligence (AI) based solution for attack detection. Used collective behavior of decentralized self-organizing swarm of nodes with simple computational rules, interacting locally. **Result:** Simple collective algorithms for detection of man in the middle attacks on data / network. The following Anomaly based attack detection algorithms were used 1. Moving average based 2. Mahalanobis distance based 3. Entropy based

		 **Use-Case:** Attack detection of attacks AMI – Smart Metering network. 1. Energy Theft by consumer. 2. Attack launched by external entity (hacker) using say man in-the-middle attack. **Technology:** Swarm Intelligence & Anomaly Based attack detection using energy consumption data from Smart Meter to detect attacks using consensus-based anomaly detection algorithms. **Solution Steps:** ▪ Each Smart meter node reads its Energy Consumption data ▪ Node shares Energy Consumption data with its neighboring nodes ▪ Node computes anomaly index based on Anomaly Detection algorithm ▪ Neighboring nodes detect anomalous node(s) based on Anomaly index by consensus ▪ Neighboring nodes raise alarm indicating attacked / compromised node ▪ Notify alarm to back end host. ▪ Display monitoring status on host UI.
Stakeholders[3]	End users of Smart Metering, Utility Companies	
Stakeholders' assets, values[4]	Competitiveness, trustworthiness, safety, privacy	

[3] Stakeholder are those that can affect or be affected by the AI system in the scenario; e.g., organizations, customers, 3rd parties, end users, community, environment, negative influencers, bad actors, etc.

[4] Stakeholders' assets and values that are at stake with potential risk of being compromised by the AI system deployment – e.g., competitiveness, reputation, trustworthiness, fair treatment, safety, privacy, stability, etc.

<table>
<tr><td>System's threats & vulnerabilities[5]</td><td colspan="4">Challenges to accountability</td></tr>
<tr><td rowspan="3">Key performance indicators (KPIs)</td><td>ID</td><td>Name</td><td>Description</td><td>Reference to mentioned use case objectives</td></tr>
<tr><td>1</td><td>Recommendation</td><td>System can be used to detect even unknown attacks in IoT Environment especially for real-time or near real-time scenarios</td><td>use-case for AMI – Smart Metering with innovative approach</td></tr>
<tr><td>2</td><td>Improve accuracy</td><td>We found the accuracy of the model to be reasonably good</td><td>Improve accuracy</td></tr>
<tr><td rowspan="5">AI features</td><td>Task(s)</td><td colspan="3">Inference</td></tr>
<tr><td>Method(s)[6]</td><td colspan="3">Machine Learning, Statistics, Heuristics, Anomaly Detection (Distance / Density based).</td></tr>
<tr><td>Hardware[7]</td><td colspan="3">IoT Nodes (like Raspberry PI, Micro-Controllers, Edge Devices, Cloud etc.</td></tr>
<tr><td>Topology[8]</td><td colspan="3">Agent based hub-spoke model.

Anomaly Detection in peer-to-peer mesh network.</td></tr>
<tr><td>Terms and concepts used[9]</td><td colspan="3">Swarm Intelligence, Anomaly Detection, AMI (Advanced Metering Infrastructure).</td></tr>
<tr><td>Standardization opportunities/ requirements</td><td colspan="4">Standardization of use of Swarm Intelligence for specific use case scenarios</td></tr>
<tr><td>Challenges and issues</td><td colspan="4">The problem is challenging because

1. Varied data set for different scenarios - large amount of data needs to be pre-processed to arrive at operation threshold parameters to be used for detection in real-time.
2. IoT (Edge) Nodes Configuration to suite specific environments The Swarm Intelligence System (SIS) involves a swarm of devices. It should be possible to easily configure the entire swarm for different network environments and locations.

Solution: Many reusable modules for Logging, Debugging and configuration through XML has been developed which has enabled</td></tr>
</table>

[5] Threats and vulnerabilities can compromise the assets and values above - e.g., different sources of bias, incorrect AI system use, new security threats, challenges to accountability, new privacy threats (hidden patterns), etc.

[6] AI method(s)/framework(s) used in development.

[7] Hardware system used in development and deployment.

[8] Topology of the deployment network architecture.

[9] Terms and concepts used here should be consistent with those defined by Working Group 1 (AWI 22989 and AWI 23053) or to be recommended for inclusion.

	binary re-use without having to change any code to suit a new network environment. 3. **Flexible to reuse / customize solution for different use-cases / scenarios and scalability** The platform needs to be able to provide facilities for different algorithms for anomaly detection to be plugged in with minimum modification, recoding, recompilation. **Solution:** Completely dynamically pluggable Algorithm binaries can be developed that conforms to defined interface Specifications, which gives flexibility to try out new algorithms, without needing to change existing code or re-compile. Use of Swarm Intelligence ensures very less localized communication that is required. Furthermore, the Swarm Intelligence System communication capability also addresses throttling of network traffic because of multi-threading / queuing capability built in.	
Societal Concerns[10]	Description	Accuracy of Solution. Fraud (Anomaly Detection) usually incurs a false positive alarm issue.
	SDGs[11] to be achieved	Responsible consumption and production

[10] To be inserted.

[11] The Sustainable Development Goals (SDGs), also known as the Global Goals, are a collection of 17 global goals set by the United Nations General Assembly. SDGs are a universal call to action to end poverty, protect the planet and ensure that all people enjoy peace and prosperity.
URL: http://www.undp.org/content/undp/en/home/sustainable-development-goals.html

Data (optional)

Data characteristics	
Description	Energy consumption data collected from smart meters.
Source[12]	1. 3 years of dataset from smart meters downloaded from publicly available data source. 2. Meter Data Sets received from IIT-Delhi. 3. Sample data collected from Smart Meter setup in the Creative Lab (C-Lab) in Samsung. 4. Analysis & Recommendations on AMI (Advanced metering infrastructure) and Smart Metering scenarios from many research papers. Various online sources on application of Swarm Intelligence as a technology for solving complex problems using simple steps.
Type[13]	Structured Data
Volume (size)	Multi-year Energy Consumption data from smart meters collected at the rate of 2 entries per hour 48 entries in a day; 17520 entries in a year.
Velocity[14]	Batch, near-real time.
Variety[15]	Single source. Similar data from multiple sources of smart meters.
Variability (rate of change)[16]	Static. Datasets vary based on geography, season etc. as energy consumption varies based on these factors.
Quality[17]	Contains some noise. Better quality after pre-processing.

12 Origin of data, which could be from customers, instruments, IoT, web, surveys, commercial activity, simulations, etc.

13 Structured/unstructured text, images, voices, gene sequences, numbers, composite: time-series, graph-structures, etc.

14 The rate of flow at which the data is created, stored, analysed, or visualized. Could be in real time.

15 Domains and types of data employed including formats, logical models, timescales, and semantics. Could be from multiple databases.

16 Changes in data rate, format/structure, semantics, and/or quality.

17 Completeness and accuracy of the data with respect to semantic content as well as syntax of the data (such as presence of missing fields or incorrect values).

Process scenario (optional)

Scenario conditions					
No.	Scenario name	Scenario description	Triggering event	Pre-condition[18]	Post-condition[19]

[18] Describes which condition(s) should have been met before this scenario happens.

[19] Describes which condition(s) should prevail after this scenario happens. The post-condition may also define "success" or "failure" conditions

Training (optional)

Scenario name	Training				
Step No.	Event[20]	Name of process/Activity[21]	Primary actor	Description of process/activity	Requirement

Specification of training data	

[20] The event that triggers the step. This might be completion of the previous event.
[21] Action verbs should be used when naming activity.

Evaluation (optional)

Scenario name	Evaluation				
Step No.	Event[22]	Name of process/Activity[23]	Primary actor	Description of process/activity	Requirement

Input of evaluation	
Output of evaluation	

[22] The event that triggers the step. This might be completion of the previous event.
[23] Action verbs should be used when naming activity.

Execution (optional)

Scenario name	Execution				
Step No.	Event[24]	Name of process/Activity[25]	Primary actor	Description of process/activity	Requirement

Input of Execution	
Output of Execution	

[24] The event that triggers the step. This might be completion of the previous event.
[25] Action verbs should be used when naming activity.

Retraining (optional)

Scenario name	Retraining				
Step No.	Event[26]	Name of process/Activity[27]	Primary actor	Description of process/activity	Requirement

Specification of retraining data	

[26] The event that triggers the step. This might be completion of the previous event.
[27] Action verbs should be used when naming activity.

References

References						
No.	Type	Reference	Status	Impact on use case	Originator/organization	Link
1	Paper	Energy Theft Detection-AMI	published	High	TSINGHUA SCIENCE AND TECHNOLOGY	https://ieeexplore.ieee.org/document/6787363/
2	Paper	Intrusion Detection - AMI	published	High	IEEE University of Illinois	https://ieeexplore.ieee.org/document/5622068/
3	Paper	EPPA	published	High	IEEE University of Waterloo, Waterloo	https://ieeexplore.ieee.org/document/6165271/
4	Report	Quantifying the Extent of Energy Theft	published	Medium	City of Cape Town, SARPA	https://www.smartenergy.com/wpcontent/uploads/Deon%20Louw_0.pdf
5	website	About Swarm Intelligence	Available Online	High	TechFerry	http://www.techferry.com/articles/swarm-intelligence.html
6						

Acceptable Reference Sources of Use Cases

— Peer-reviewed scientific/technical publications on AI applications (e.g. [1]).
— Patent documents describing AI solutions (e.g. [2], [3]).

— Technical reports or presentations by renowned AI experts (e.g. [4])
— High quality company whitepapers and presentations
— Publicly accessible sources with sufficient detail

This list is not exhaustive. Other credible sources may be acceptable as well.

Examples of credible sources:

— [1] B. Du Boulay. "Artificial Intelligence as an Effective Classroom Assistant". IEEE Intelligent Systems, V 31, p.76–81. 2016.
— [2] S. Hong. "Artificial intelligence audio apparatus and operation method thereof". N US 9,948,764, Available at: https://patents.google.com/patent/US20150120618A1/en. 2018.
— [3] M.R. Sumner, B.J. Newendorp and R.M. Orr. "Structured dictation using intelligent automated assistants". N US 9,865,280, 2018.
— [4] J. Hendler, S. Ellis, K. McGuire, N. Negedley, A. Weinstock, M. Klawonn and D. Burns. "WATSON@RPI, Technical Project Review".
URL: https://www.slideshare.net/jahendler/watson-summer-review82013final. 2013.