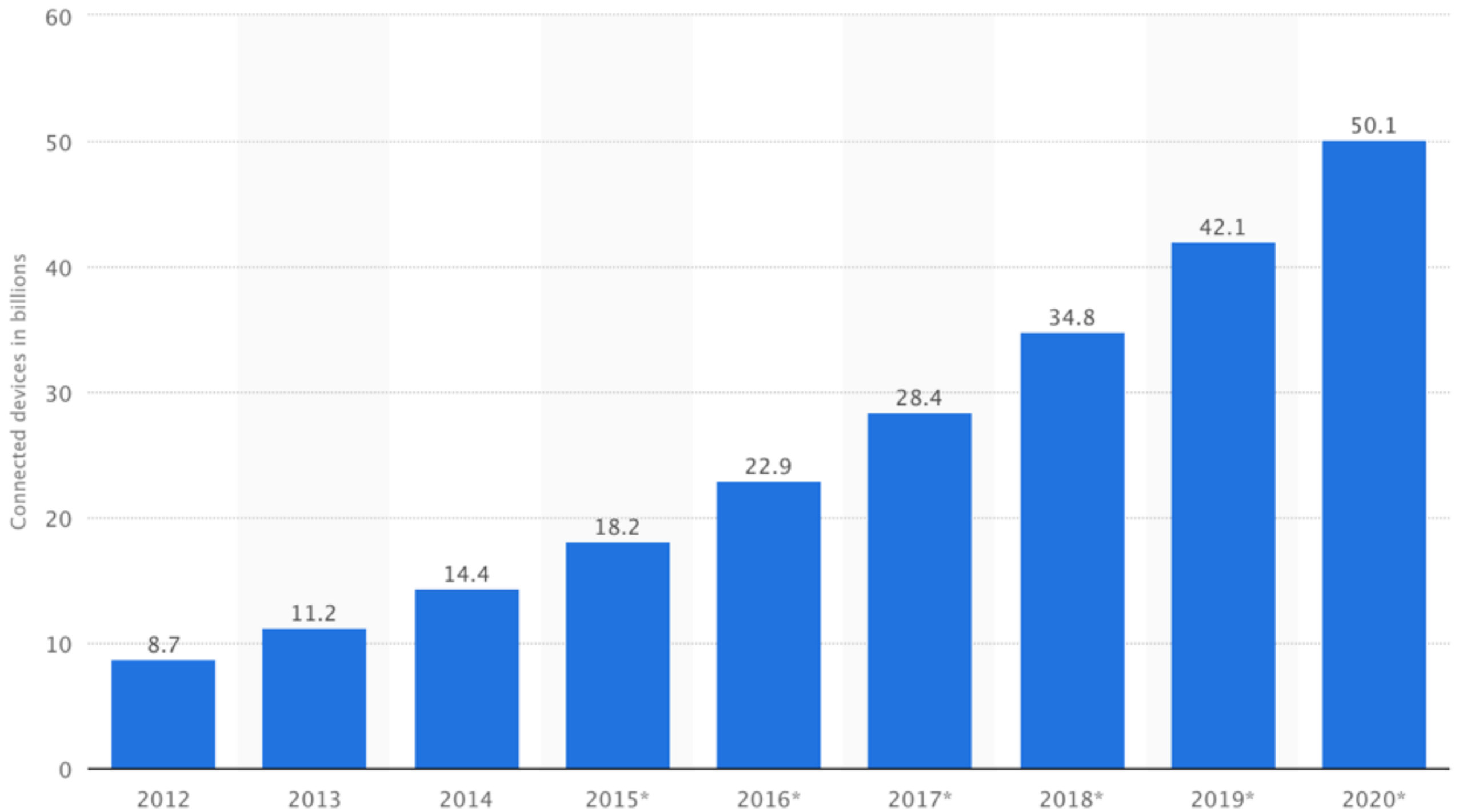# Apparatus: Reasoning about security requirements in IoT

By Orestis Mavropoulos, Haralambos Mouratidis, Andrew Fish, Emmanouil Panaousis, Christos Kalloniatis
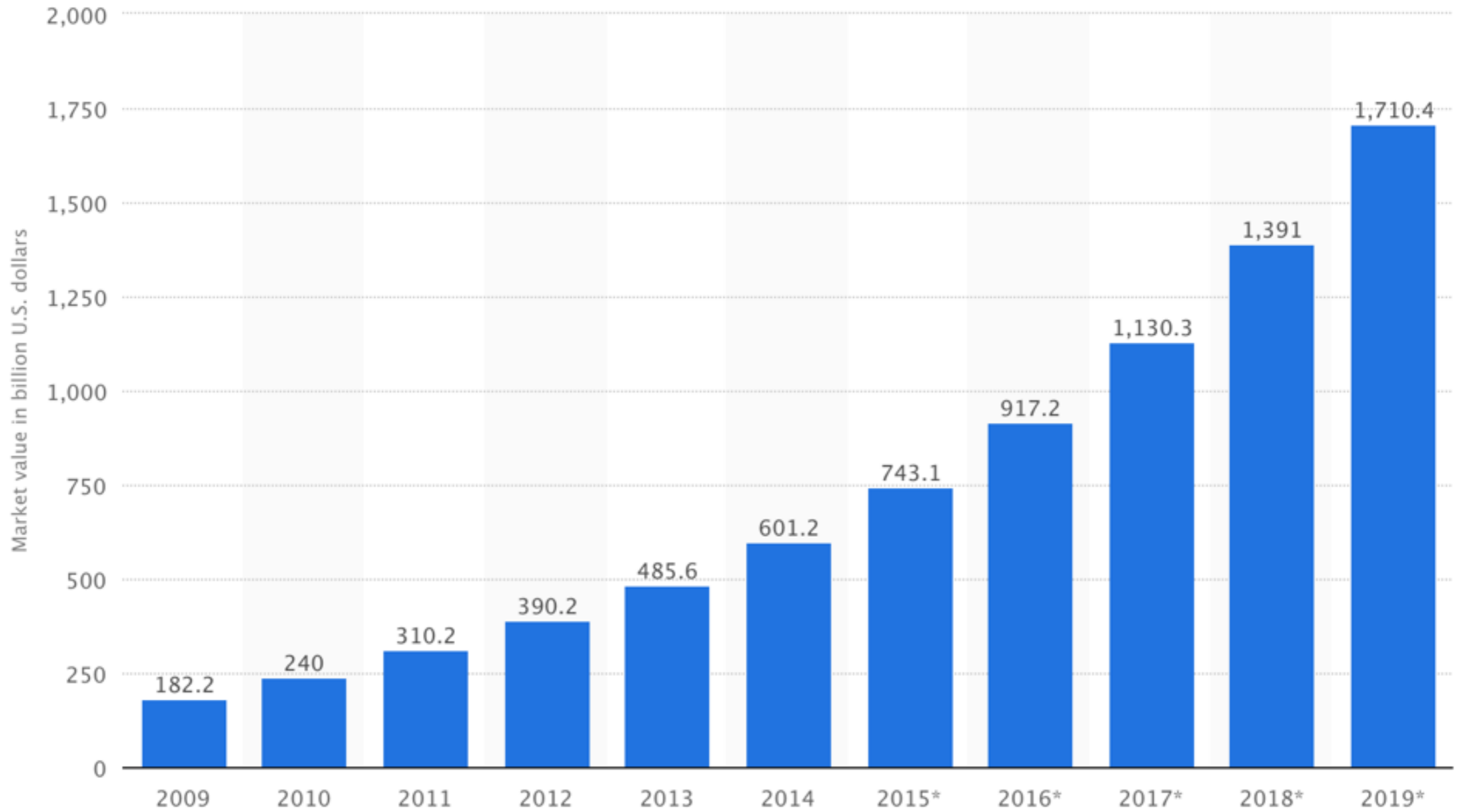
University of Brighton, United Kingdom
University of Aegean, Greece

"A network that not only connects people but also objects around them."

–Kevin Ashton

Connected devices

Market value

Research challenges in IoT

- Lack of standards.

- Explosive growth rate.

- Scale of networks.

Security challenges of IoT

- Vulnerability inheritance.

- Update management and maintenance.

- Sensors as a service.

- Connection of cyber attacks to physical ones.

- Largest attack surface.

What is Apparatus?

- Exploratory method.

- Security elicitation from the architecture of an IoT system.

- Modular functionality.

- Security analysis is semi-automated.

- Information is presented in JSON format.

Key concepts of Apparatus

- IoT node: any device that needs to be represented as part of an Internet of Things system. A device has a set of properties that describe its role in the system.

- Network connection: how devices exchange data.

- Microworld: a managed/controlled environment that constitutes a collection of IoT nodes necessary for an IoT system to function.

IoT node properties

- Identification: Stakeholders (user, deployer, developer, manufacturer)

- Aspect: physical or virtual

- Layer: application, gateway, perception

- Type: device represented

- Attribute: functionality of the node

- Input & Output: required/outputted data
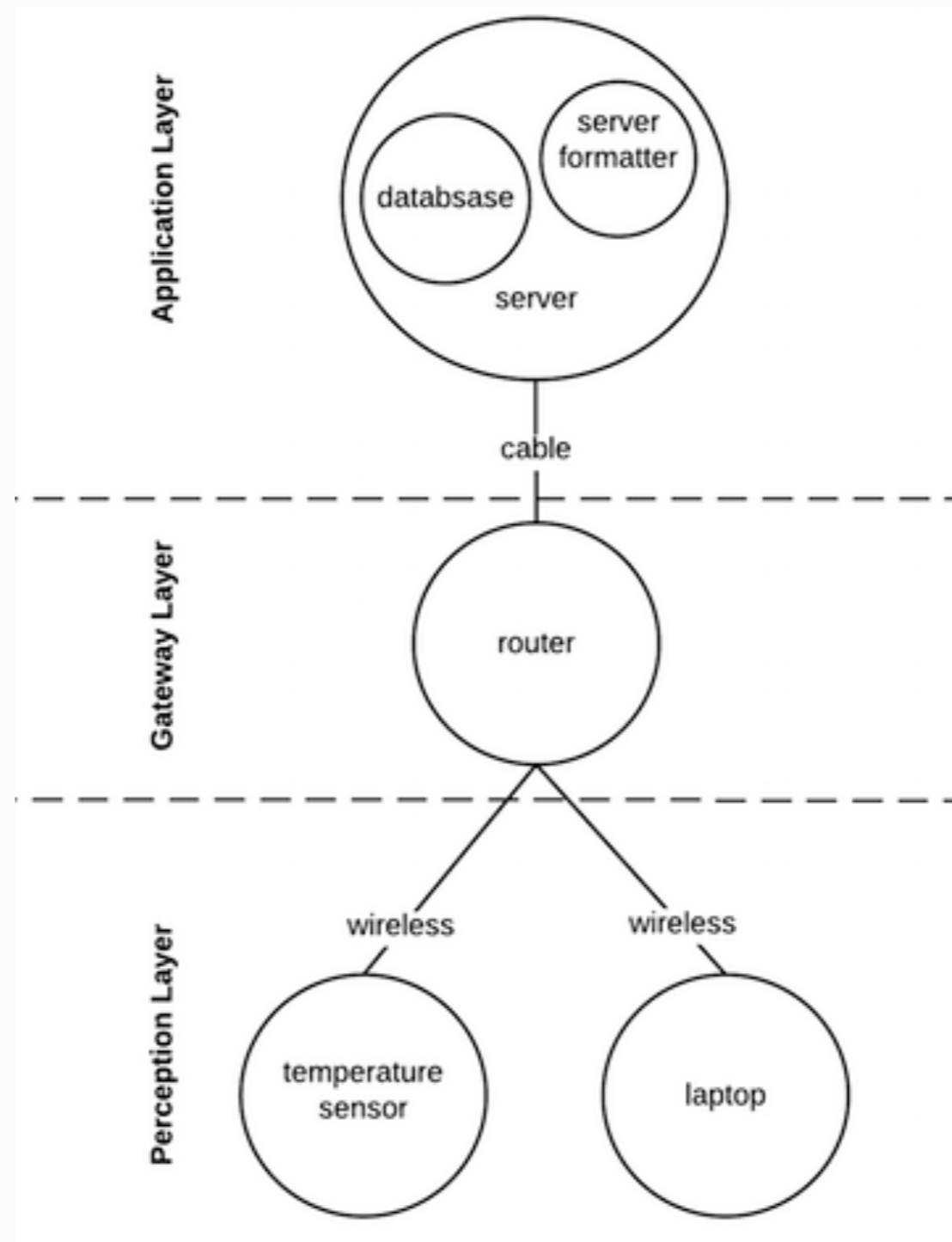
Network Connection properties

- Wireless: Wi-Fi, Bluetooth, NFC, etc

- Cable: ethernet, USB, etc
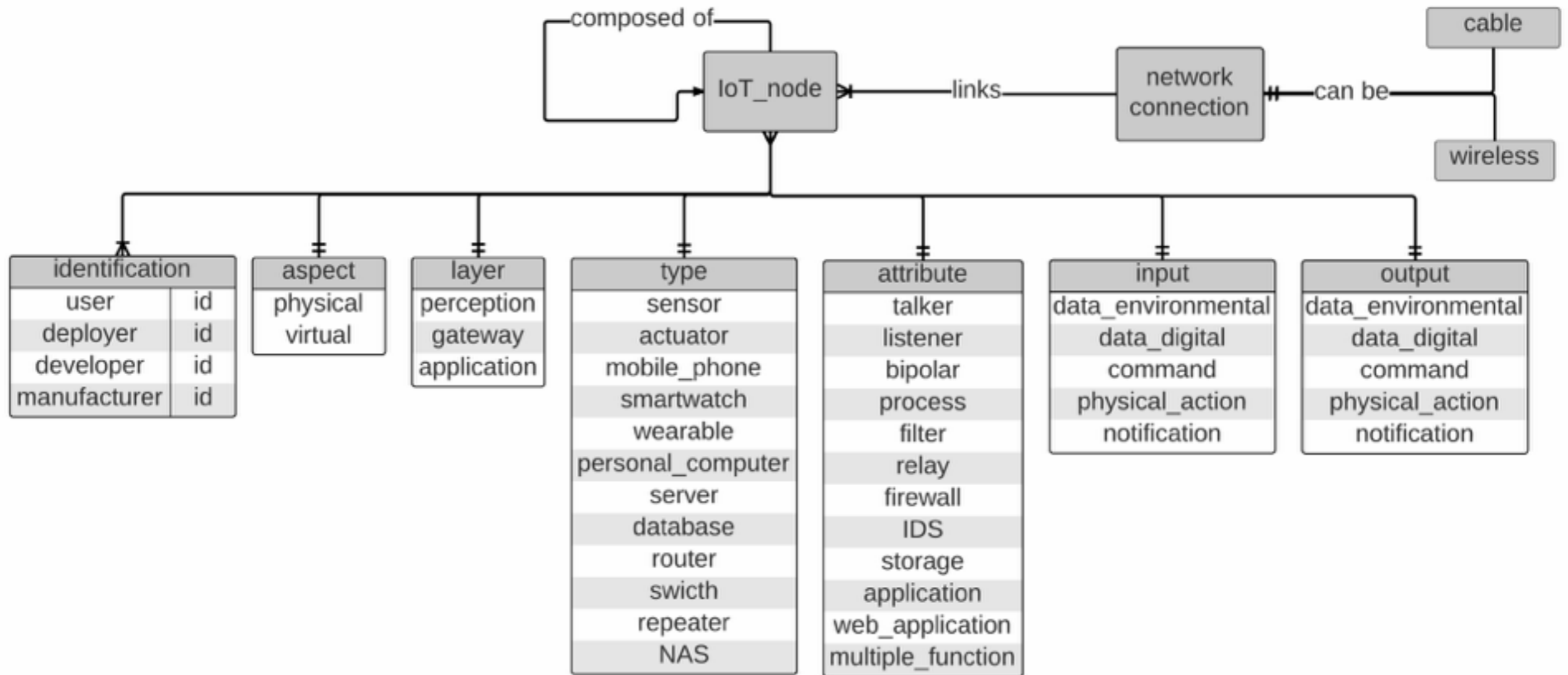
Conceptual model

JSON Skeleton Schema

```json
{
    "IoT_system": [{
        "IoT_node_01": [{
            "identification": {
                "user": " ",
                "deployer": " ",
                "developer": " ",
                "manufacturer": " "
            },
            "aspect": " ",
            "type": " ",
            "attribute": " ",
            "input": " ",
            "output": " ",
        }, {
            "connection": {
                "connects_to": "node_name",
                "connection_type": " "
            }
        }]
    }]
}
```

Temperature monitoring IoT system

```json
1  {
2    "IoT_system": [{
3      "sensor": [{
4        "identification": {
5          "user": "01",
6          "deployer": "01",
7          "developer": "02",
8          "manufacturer": "02"
9        },
10        "aspect": "physical",
11        "layer": "perception",
12        "type": "sensor",
13        "attribute": "talker",
14        "input": "data_environmental",
15        "output": "data_digital"
16      }, {
17        "connection": {
18          "connects_to": "router",
19          "connection_type": "wireless"
20        }
21      }]
22    },
23    {
24      "router": [{
25        "identification": {
26          "user": "01",
27          "deployer": "01",
28          "developer": "02",
29          "manufacturer": "02"
30        },
31        "aspect": "physical",
32        "layer": "gateway",
33        "type": "sensor",
34        "attribute": "relay",
35        "input": "data_digital",
36        "output": "data_digital"
37      }, {
38        "connection": {
39          "connects_to": "server",
40          "connection_type": "cable"
41        }
42      }]
43    }, {
44      "server": [{
45        "identification": {
46          "user": "01",
47          "deployer": "01",
48          "developer": "02",
49          "manufacturer": "02"
50        },
51        "aspect": "physical",
52        "layer": "application",
53        "type": "server",
54        "attribute": "multiple_function",
55        "input": "data_digital",
56        "output": "data_digital"
57      }, {
58        "connection": {
59          "connects_to": "router",
60          "connection_type": "cable"
61        }
62      }]
63    }, {
64      "database": [{
65        "identification": {
66          "user": "01",
67          "deployer": "01",
68          "developer": "02",
69          "manufacturer": "02"
70        },
71        "aspect": "virtual",
72        "layer": "application",
73        "type": "database",
74        "attribute": "storage",
75        "input": "data_digital",
76        "output": "data_digital"
77      }, {
78        "connection": {
79          "connects_to": "router",
80          "connection_type": "cable"
81        }
82      }]
83    }, {
84      "server_formatter": [{
85        "identification": {
86          "user": "01",
87          "deployer": "01",
88          "developer": "02",
89          "manufacturer": "02"
90        },
91        "aspect": "virtual",
92        "layer": "application",
93        "type": "server",
94        "attribute": "process",
95        "input": "data_digital",
96        "output": "data_digital"
97      }, {
98        "connection": {
99          "connects_to": "router",
100         "connection_type": "cable"
101       }
102     }]
103   }, {
104     "laptop": [{
105       "identification": {
106         "user": "01",
107         "deployer": "01",
108         "developer": "02",
109         "manufacturer": "02"
110       },
111       "aspect": "physical",
112       "layer": "perception",
113       "type": "laptop",
114       "attribute": "listener",
115       "input": "data_digital",
116       "output": "notification"}, {
117       "connection": {
118         "connects_to": "router",
119         "connection_type": "wireless"
120       }
121     }]
122   },
123   ]
124 }
```

Temperature monitoring system in JSON format

```json
1  {
2    "IoT_system": [{
3        "sensor": [{
4          "identification": {
5            "user": "01",
6            "deployer": "01",
7            "developer": "02",
8            "manufacturer": "02"
9          },
10         "aspect": "physical",
11         "layer": "perception",
12         "type": "sensor",
13         "attribute": "talker",
14         "input": "data_environmental",
15         "output": "data_digital"
16       }, {
17         "connection": {
18           "connects_to": "router",
19           "connection_type": "wireless"
20         }
21       }]
22     },
23     {
24       "router": [{
25         "identification": {
26           "user": "01",
27           "deployer": "01",
28           "developer": "02",
29           "manufacturer": "02"
30         },
```

```json
63     }, {
64       "database": [{
65         "identification": {
66           "user": "01",
67           "deployer": "01",
68           "developer": "02",
69           "manufacturer": "02"
70         },
71         "aspect": "virtual",
72         "layer": "application",
73         "type": "database",
74         "attribute": "storage",
75         "input": "data_digital",
76         "output": "data_digital"
77       }, {
78         "connection": {
79           "connects_to": "router",
80           "connection_type": "cable"
81         }
82       }]
83     }, {
84       "server_formatter": [{
85         "identification": {
86           "user": "01",
87           "deployer": "01",
88           "developer": "02",
89           "manufacturer": "02"
90         },
91         "aspect": "virtual",
92         "layer": "application"
```

Temperature monitoring system in JSON format

Example of Security Requirements Elicitation

- Nodes should be physically protected -> lines 11, 112 (layer:perception)

- Environmental data should not tamper with the system -> line 14 (input:data_environmental)

- System can only be used by authorised users and devices -> line 19 (connection:wireless)

Future Work

- Introduce more modules in Apparatus (network, security, social)

- Automate the process of security requirement elicitation.

- Provide automated security adaptability.

- Incorporate other security requirements engineering methodologies as modules.

Thank you for listening.

-orestis