**IBM Watson IoT Platform**

This Service Description describes the Cloud Service. The applicable order documents provide pricing and

additional details about Client's order.

**Cloud Service**

IBM Watson IoT Platform connects devices, ingests device data and transforms that data into meaningful

insights. Watson IoT Platform and its additional add on services enable Clients to capture data for

devices, equipment, and machines, to explore this data, and to discover insights on this data that drive

better decision making. Watson IoT Platform provides a pre-integrated foundation for industry solution

and Client applications built on IoT data.

IBM Watson IoT Platform is made up of three fundamental services: Connection Service, Analytics

Service, and Blockchain Service. All three services have a nonproduction package for proofs of concept

and pilot work, as well as a production package for full production deployment.

IBM Watson IoT Platform Connection Service capabilities include:

● Connection of a wide spectrum of IoT devices

● IoT device registration and management

● User Registration, setup, and authentication

● Ability to create alerts

● Security with TLS authentication support, access control group for devices & gateways

● Data Lifecycle Management

● Solution administration for deployment and device groupings

Additionally:

● Analytics Service enable to enrich, augment and interact with raw data

● Blockchain Service enable to connect with Blockchain enabled networks

**Offerings**

The Client may select from the following available offerings.

IBM Watson IoT Platform – Connection Service Sensor

This Cloud Service is intended to be used by "Sensor" class devices which include low cost sensors, parking meters, and street lights. The following table shows the consumption included in this Cloud Service per Sensor Client Device.

**Node Red Service**

Trigger-Action Platforms (TAPs) play a vital role in fulfill-ing the promise of the Internet of Things (IoT) by seamlessly connecting otherwise unconnected devices and services. While enabling novel and exciting applications across a variety of services, security and privacy issues must be taken into consideration because TAPs essentially act as persons-in-the-middle between trigger and action services. The issue is further aggravated since the triggers and actions on TAPs are mostly pro- vided by third parties extending the trust beyond the platform providers. Node-RED, an open-source JavaScript-driven TAP, provides the oppor- tunity for users to effortlessly employ and link nodes via a graphical user interface. Being built upon Node.js, third-party developers can extend the platform’s functionality through publishing nodes and their wirings,

known as flows.

This paper proposes an essential model for Node-RED, suitable to rea-son about nodes and flows, be they benign, vulnerable, or malicious.We expand on attacks discovered in recent work, ranging from exfil - trating data from unsuspecting users to taking over the entire platform by misusing sensitive APIs within nodes. We present a formalization of a runtime monitoring framework for a core language that soundly and transparently enforces fine-grained allowlist policies at module-, API-, value-, and context-level. We introduce the monitoring framework for

Node-RED that isolates nodes while permitting them to communicatevia well-defined API calls complying with the policy specified for each

**Cloudant DB**

IBM provides IBM Cloudant data hosting services (the "Hosting Services") to you ("you" and "your" or "Subscriber") (Cloudant and Subscriber each a "Party" and collectively "Parties") subject to the following Terms of Service. In order to use the Hosting Services,you must first agree to lthese Terms of Service. You may not use the Hosting Services if you do not accept these Terms of Service. You can accept these Terms of Service by (i) clicking "I ACCEPT" where this option is made available to you in the user interface; or (ii) by accessing and using the Hosting Service, in which case you understand and agree that Cloudant will treat your use of the Hosting Services as acceptance of these Terms of Service from that point onwards. Changes to these Terms of Service IBM may make changes to these Terms of Service from time to time. When these changes are made, Cloudant will make a revised version of these Terms of Service available acloudant.com/terms. You understand and agree that if you use the Hosting Services after the date on which these Terms of Service have changed, IBM will treat your continued use as acceptance of the revised Terms of Service.Persons Not Eligible to Use the Hosting Services .