Centre of Innovation for IoT/M2M

सी-डॉट
C-DOT

Contents

Figures

Centre of Innovation (COI) for M2M

1 Scope

C-DOT is setting up a Centre of Innovation for collaborating with the industry for development and deployment of solutions using Internet of Things/Machine to Machine technologies. This center will assist in development, integration and testing of innovative Smart Solutions based on oneM2M standards. OneM2M standards have been transposed as national standards for IoT/M2M in India. The center will bring together various industry partners to create an end-to-end solution like smart city solution. This document provides details of the engagement with the industry and is useful for organisations interested in creating National Standards compliant indigenous IoT/M2M solutions.

2 Background

During the last two decades, the availability of affordable sensors, together with the proliferation of internet infrastructure enabled an interesting technology called the Internet of Things (IoT) which has also been known as Machine-to-Machine Communication(M2M). Riding on the advancement in sensor and communication technologies, IoT/M2M is continuously changing almost every aspect of present-day life. The continuous increase in number of connected devices and the huge growth of connected devices projected in the coming years, shows that M2M is the future technology that is here to stay and will proliferate in multiple sectors. In the past few years, worldwide growth in Internet usage and broadband (with declining costs) have given a boost to IoT/M2M. According to Statista, the number of IoT devices worldwide is forecast to almost triple from 8.74 billion in 2020 to more than 25.4 billion IoT devices in 2030. In 2020, the highest number of IoT devices were found in China (3.17 billion devices).

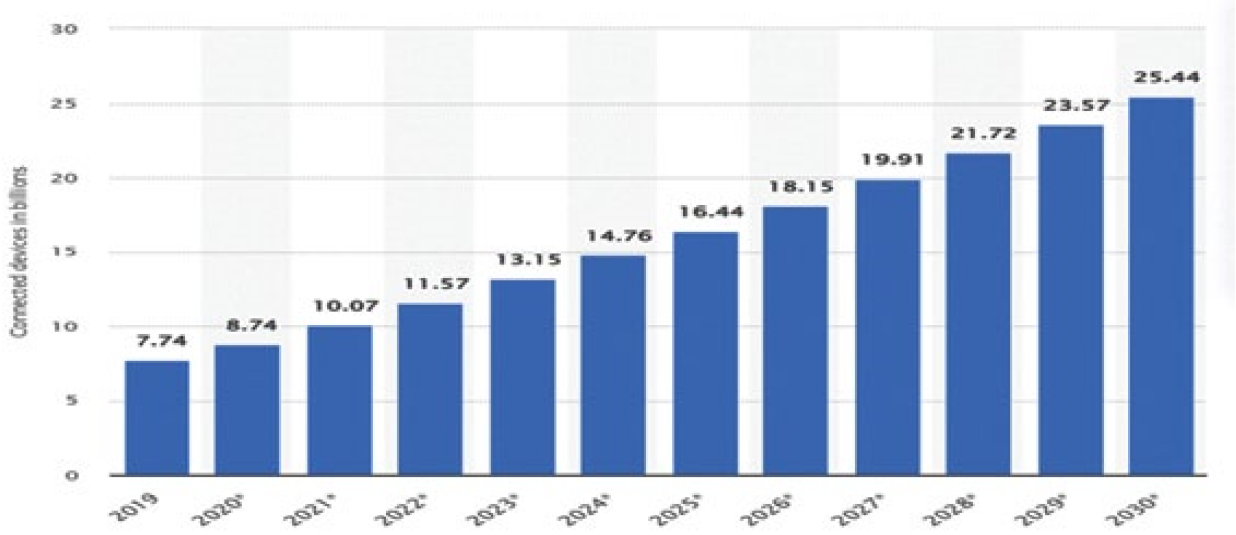


Figure 1:Worldwide growth rate of IoT devices

However, the deployment of IoT/M2M solutions continue to happen in siloed, vertical centric fashion. As a result, the ecosystem has been flooded with several proprietary IoT/M2M platforms/solutions like one for transport, other for smart street lights, another for waste management and so on. Such proliferation of proprietary implementations has trapped the users in a vendor locked-in situation where neither there is any scope for interoperability of devices/applications nor does it allow data sharing between divergent applications *(Refer Annexure A: Siloed Implementations – Issues and Challenges)*.

The practitioners as well as the users of IoT applications have understood the fact that the real value of IoT comes when the devices and applications become seamlessly interoperable, secured sharing of data produced by the sensors becomes possible while maintaining the privacy and development of innovative applications become easier and faster (Refer An*nexure B: The Common Essential needs of all IoT/M2M Applications).*

Isolated solutions not only inhibit sharing of data for increased efficiency but also lead to increased CAPEX and OPEX.*(Refer Annexure C :Examples of data sharing).*

As the ecosystem is expected to experience massive growth, lack of standardization in IoT/M2M deployments will have a direct impact on the Total Cost of Ownership (TCO). Thus, from the futuristic viewpoint, it is necessary to have standardized deployments of IoT/M2M solutions.

3 CCSP (C-DOT Common Service Platform)

C-DOT has been the flagbearer of IoT/M2M standardization and has been contributing significantly to oneM2M - the global IoT/M2M standard *(Refer Annexure D : About oneM2M)*. C-DOT is one of the largest contributors in oneM2M with more than 400 technical contributions so far. Release 2 of oneM2M specifications has been adopted by DoT as the National Standard for IoT/M2M. C-DOT has a state-of-the-art oneM2M compliant C-DOT Common Service Platform (CCSP) which can help in standards based M2M solutions deployment in the country. C-DOT Common Service Platform (CCSP), is the horizontal IoT/M2M platform based on oneM2M *(Refer Annexure E: C-DOT Common Service Platform – CCSP)*. The USP of CCSP is in the Common Services Entity (CSE), which sits below the M2M application layer and above the transport layer.

C-DOT is known for its legacy of promoting a viable ecosystem that is beneficial for the country and it is aiming to achieve the same in the area of IoT/M2M. C-DOT Centre of Innovation (COI) for IoT/M2M is being setup in which the standardized interfaces of the CCSP Platform would be opened for the organizations (especially Startups) developing indigenous IoT/M2M applications for testing their IoT/M2M solutions with CCSP and working out end to end solutions for various industry verticals. The Centre of Innovation shall provide a playground for the Indian Startups and Industry to collaborate with each other to build and deploy innovative, interoperable, secure and scalable solutions based on oneM2M, the National IoT/M2M Standard and thus providing a fillip to the objectives of Atmanirbhar Bharat.

C-DOT's Delhi Campus would be hosting the infrastructure for the CCSP platform as a private cloud which would be accessible over the internet in a secured manner for the selected industry partners.

4 Objective of the Centre of Innovation

As mentioned above, majority of the vendor locked-in proprietary implementations of IoT/M2M including those in the Indian Smart Cities have been done using proprietary technologies *(Refer Annexure F : M2M enabled Smart Cities)*. Indian IoT/M2M organisations including startups, have not been able to contribute significantly in these endeavors despite being significantly innovative with their solutions. C-DOT, with the launch of Centre of Innovation for IoT M2M, aims to solve the prevailing issues of the IoT/M2M ecosystem with CCSP as it meets all the essential requirements of IoT/M2M solutions.

The main objectives of the COI are as following:

1. To create an ecosystem of indigenous solution developers and system integrators for development and deployment of oneM2M standards compliant IoT/M2M solutions
2. To provide an easy to use facility for testing the solutions developed by IoT/M2M solution providers and system integrators and help them bridge the gap to make them oneM2M compliant.
3. To create synergies among the Startups and M2M/IoT Industry for capacity building in the area of oneM2M standards-based products and applications.
4. To bridge the gap between R&D and commercialization of oneM2M standards based M2M/IoT products
5. To create successful startups in the area of IoT/M2M
6. To promote innovations in the area of IoT/M2M

After successful testing of the application, the parties would be encouraged to become part of a consortium to target the market together. For this purpose, the parties would be required to sign the Memorandum of Understanding (MoU). However, this would not be binding for any party engaged in this exercise and they would be free to exit from the engagement at any point in time.

5 Functions of the Centre of Innovation

- Evaluate the IoT/M2M applications for its compliance to national standards and readiness for the market.
- Provision for technical assistance to the selected parties towards integration and testing their solutions with CCSP and making it compliant to National Standard.
- The Centre of Innovation would provide an environment for the IoT device manufactures and application providers to utilize the features of C-DOT Common Service Platform (CCSP) to create National standards compliant innovative applications and solutions.
- Industry partners can leverage Centre of Innovation setup for:
  - Development of interoperable applications with respect to National IoT/M2M Standard i.e., oneM2M specifications
  - Utilizing the testing infrastructure for testing the products and applications
  - Collaboration with C-DOT for commercial bidding in future IoT/M2M tenders
  - Widening their commercial horizons.
- Provide certificate to parties for the successful development and testing of their oneM2M compliant solutions with CCSP.

6 Proposed Verticals

The Centre of Innovation will accept the proposal for any IoT/M2M application that meets the requirement of any domain/vertical. However, to start with following verticals will be given priority in order to develop complete National Standards compliant solutions for Smart Cities:

- Asset Tracking
- Transport
- e-Health
- Environment
- Surveillance
- Solid Waste Management
- Smart Metering (Gas/Water)
- Safety and Security (including Fire detection, prevention and healthiness monitoring)
- Smart Home
- Active Assisted Living

Besides Smart Cities, other viable solutions including those for the rural sector would also be considered.

The following figure illustrates the architecture of the COI setup for development and testing.

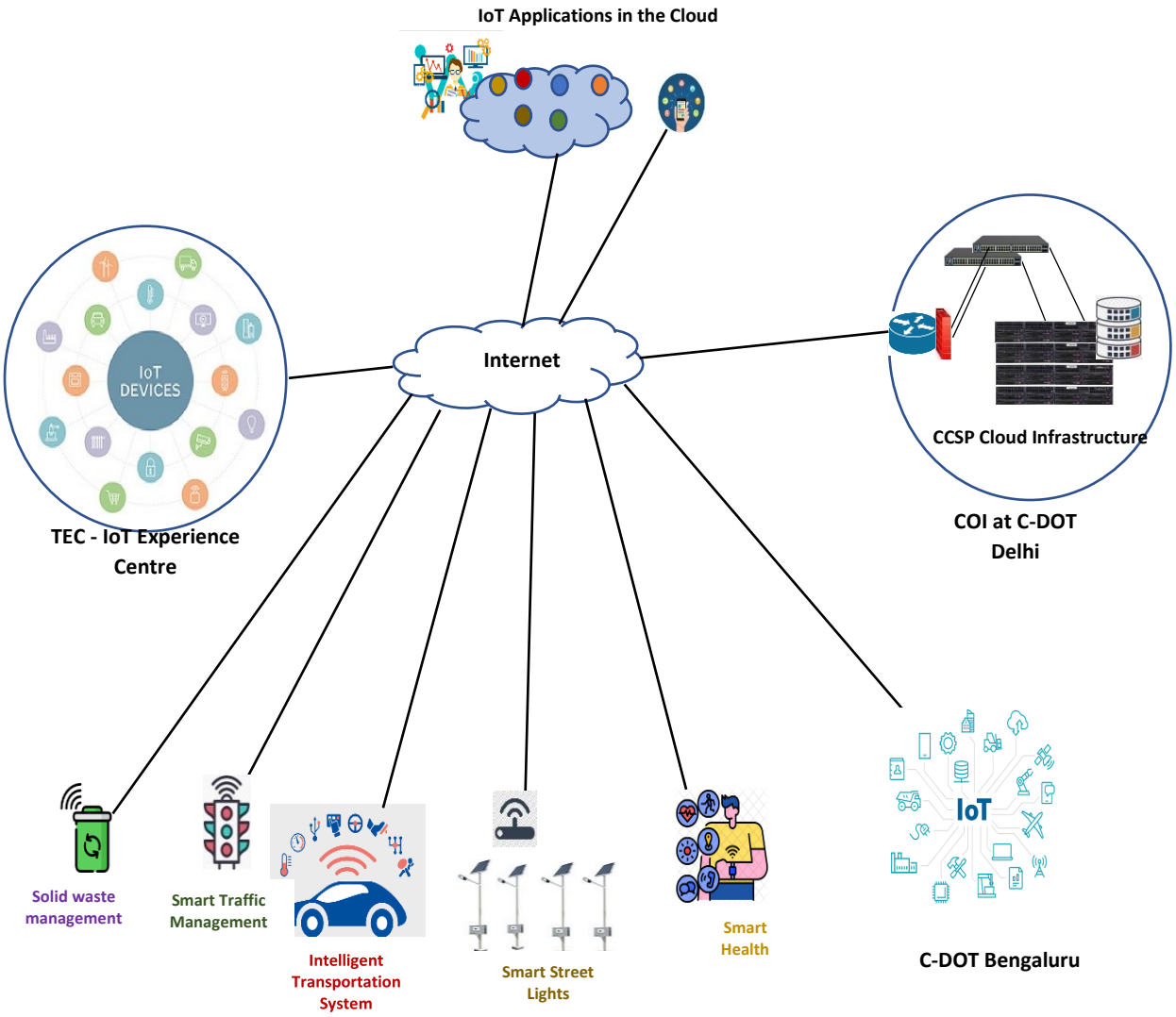


Figure 2: National Standard based IoT/M2M architecture around Centre of Innovation

As mentioned above, the COI infrastructure will be setup at the C-DOT Delhi Campus and will be accessible over the internet. The selected Industry partners can connect to the CCSP from any location. However, only registered and authenticated devices/applications would be allowed to communicate with CCSP in a secured manner. In case the industry partner wishes to demonstrate their products/solutions physically, the same can be done at any of the three sites i.e., C-DOT

Delhi Campus, C-DOT Bengaluru Campus & IoT Experience Centre in Telecom Engineering Centre, Delhi subject to feasibility.

7 Funding

COI would not be providing any funding for engagement. However, funding may be considered through other schemes of C-DOT/DoT for startups. COI would provide the necessary technical know how and assistance towards testing, integration and development without any charge. The complete testing infrastructure will be thrown open to the IoT/M2M application/service providers. Space and electrical power etc. to develop and test the solutions with CCSP will be considered on receipt of a formal communication from the startups on case to case basis.

8 Intellectual Property Rights

Any and all intellectual property created solely in relation to or arising out of this engagement, by industry partners during the validity of the engagement, or prior to the engagement, or after the termination of the engagement shall be under the sole and exclusive ownership of the industry partners.

Any intellectual property created solely in relation to or arising out of this engagement, by C-DOT during the validity of the engagement, or prior to the engagement, or after the termination of the engagement shall be under the sole and exclusive ownership of the C-DOT.

Ownership of any and all intellectual property created / developed jointly through collaborations under this engagement will be determined between the Parties through mutual consultation and recorded in writing as an addendum/amendment/agreement separately on a case- to -case basis.

9 How to Apply

Interested organisations should visit the website https://coi.cdot.in. The details about the onboarding, testing etc. along with Frequently Asked Questions (FAQs) about the CCSP platform are available.

The interested organisations are required to fill the online application form available by clicking the “Register for Testing” link.

A copy of the sample form is enclosed in Annexure G.

Any further queries may be sent to **coi@cdot.in**

10 Selection Process

The selection of the industry partners (hereinafter referred as parties) would be done by a Screening Committee (SC) consisting of the following members:

S. No.	Member	Role in Committee
1.	Director, C-DOT*	Chair
2.	DDG, DoT	Member
3.	DDG, TEC	Member
4.	Head, IPR, C-DOT	Member
5.	Group Heads/Staff of IoT/M2M Groups, C-DOT	Member
6.	Experts from Academia and Industry	Member(s)

*Director may also nominate an expert as Chair

The selection of the parties would primarily depend upon the following parameters:

S. No.	Criteria	Description
1.	Background of the Organisation	Organisations having expertise in development or delivery of IoT/M2M solutions/services
2.	Relevance of the application area	Relevance of the IoT/M2M application from the perspective of deployment in Smart Cities/Consumer IoT/Smart Health/Energy Sector/Intelligent Transport/Rural sector etc.
3.	Innovative approach	Innovation in the proposed solution/ Unique proposition
4.	Scalability of the solution	Scalability of the solution from technology as well as business perspective
5.	Adherence to National standard	Degree of compliance to National Standard (oneM2M) for IoT/M2M
6.	Market focus	Business potential market acceptability

The applicants shortlisted based on the above criterion would be required to give presentations before the committee on their solutions. The committee would select the startups/organizations for participation in COI.

11 Who should apply:

A. Startups, as defined and recognized by Department for Promotion of Industry and Internal Trade (DPIIT), Ministry of Commerce and Industry, Government of India, working towards innovation, development or improvement of M2M/IoT ecosystem or services. Startups /MSMEs who have already tested their prototypes (hardware/software innovations) with or without using any oneM2M standard platform.

B. Any Indian company incorporated under the Companies Act 1956/2013, having over 51% stakes by the Indian Citizen / NRI / OCI and Head Quarter in India and interested in the development, testing and integration of IoT/M2M applications with National Standards based platforms.

C. M2M/IoT service providers interested in joining the consortium for creating end-to-end solutions and commercial bidding in future IoT/M2M tenders.

D. Organisations seeking further validations with CCSP platform before becoming market-ready

12 On-boarding Applications on CCSP

1. Interested parties shall follow the link on COI Portal (https://coi.cdot.in) and click on "Register for Testing" link and fill in the details in the online registration form.
2. Based on the details filled, the Screening Committee (SC) would shortlist the parties who have registered for collaboration.
3. The shortlisted parties would be notified by mail about their onboarding process.
4. The parties would be required to sign the Non-Disclosure Agreement (NDA) for collaboration with C-DOT. The NDA formalities along with the form will be shared with the parties over e-mail.
5. The parties have to sign the NDA and send it to C-DOT.
6. On completion of the NDA formalities the parties will be provided with the link to fill in the application and device details.
7. Scope of testing and timeframes will be fixed.
8. M2M Service Subscription will be provisioned on CCSP according to the details given for the application.
9. Service Subscription will be activated for testing.

10. Digital Certificates will be generated by the Certificate Authority Server and the parties would be required to download the same.
11. Thereafter, the parties can start testing their applications.
12. In case the parties need to make changes in their code for successful integration, they will be given a time of one month. The maximum duration for development & testing would be 6 months.
13. Test Report will be generated and submitted to the Screening Committee.
14. Certificate will be given to the party on successful integration testing on recommendation of SC. The party would be listed in the CDOT website as a successful integrator for a particular release of oneM2M standard.
15. After testing, the parties would be invited to join a consortium with C-DOT as recommended by the committee. They would also be encouraged to deploy their solutions in the COI experience centers at C-DOT Delhi and/or Bengaluru.

13 Exit Criteria

Each party shall be entitled to exit this engagement, by operation of law and without demand, immediately; in case of material breach of this engagement by the other party if the defaulting Party has not remedied such breach within thirty (30) days of receiving such notice to cure the default.

This engagement shall terminate by operation of law and without demand, upon first occurrence of one or more of the following events:

i. Mutual written agreement of the Parties to terminate the engagement
ii. Expiry of six months from the Effective Date of this engagement unless otherwise agreed by the Parties to extend it beyond this expiry date
iii. If either Party is prohibited under prevalent rules or notifications or laws from the relevant administration
iv. Any breach of contract

In such cases no Party shall incur any liability whatsoever.

Annexures

Annexure A : Siloed Implementations: Issues and Challenges

From the Smart Solutions perspective, the major use cases implemented in majority of the global smart cities are connected public transport, traffic monitoring and management, water level / flood monitoring, video surveillance and analytics, connected streetlights, weather monitoring, air quality / pollution monitoring, smart metering – water/electricity, fire / smoke detection and water quality monitoring etc.

The typical architecture adopted for the deployment of these smart solutions is given in the figure below.

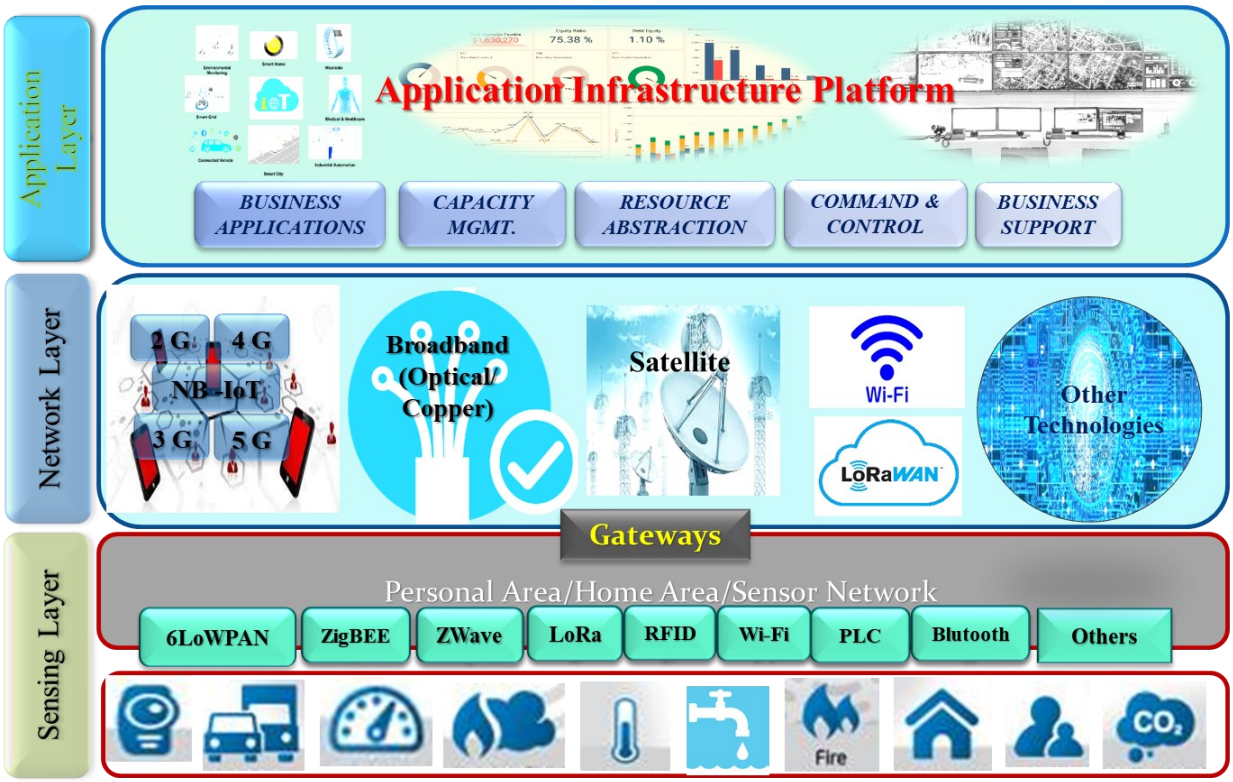
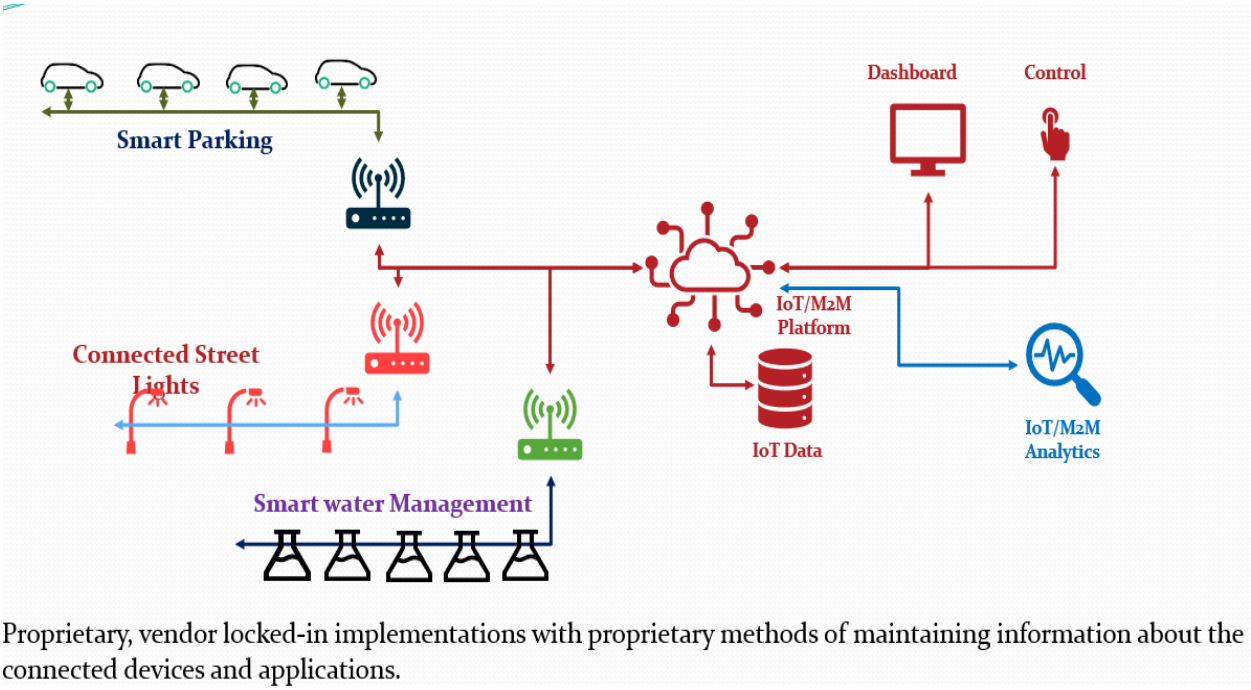


Figure 3: Typical Architecture of Smart City IoT Applications

The sensing layer contains the sensors and actuators which connect to the gateways using any of the Personal Area Network (PAN) technologies like Zigbee, 6LowPAN, Bluetooth and LoRa etc. The gateway devices typically connect using any network technologies shown in the Network Layer to the Application Infrastructure Platform shown in the Application Layer. The information pertaining to the sensors, actuators, gateways etc. are tightly coupled with the Application Layer entities.

The solutions mentioned above have mostly been deployed using proprietary IoT Platforms which control the onboarding of such applications and require substantial integration efforts for such purposes. The deployment scenario has been illustrated in the following figure.



Proprietary, vendor locked-in implementations with proprietary methods of maintaining information about the connected devices and applications.

Figure 4: Deployment of Smart Solutions in Smart Cities

However, owing to the proprietary, non-standardised deployment of solutions, the implementation of these so called 'Smart Solutions' create issues like lack of interoperability, proprietary methods of data sharing, vendor-lock-in and inadequate or non-existent security etc. Where on one hand the ecosystem is expected to experience massive growth, the industry and the authorities both are concerned about the issues and challenges arising due to lack of standardization.

Annexure B : The Common Essential needs of all IoT/M2M Applications

In order to have a cost effective and efficient deployment of IoT/M2M Applications, irrespective to their types and target consumer, the following features are essential-

Interoperability

As has been mentioned earlier that in order to have a sustainable large-scale deployment of IoT/M2M Solutions, it is essential to have interoperability of applications, devices, networks and also semantics. The solutions would not be free from vendor lock-in if such interoperability is not achieved in these solutions. In practice, no city deploys solutions across pan city in one go. Rather, the solutions are deployed in phased manner in an Area Based Development (ABD) model. For example, Smart Street Light solutions deployed in one part of the city may not be the best choice in later phases owing to another competing solution being more feature rich, more efficient or giving better price advantage. However, due to lack of interoperability the cities are forced to stick to the older model.

Security and Privacy

Device Security, Authentication, Authorisation, Communication Security, Data Integrity, Data Privacy and Lawful Interception etc. are the essential requirements for IoT/M2M deployments. Therefore, it is necessary that a standardized practice of robust security framework be mandated for all IoT/M2M deployments which do not escape the regulations for mandatory testing and certification.

Deployment of only authorized devices and applications

In IoT/M2M Solutions, the sensors and actuators play the most vital role i.e., the role of "data generators" and that of "Acting upon it" respectively. Needless to say, the situation can be catastrophic if these are compromised. It is therefore necessary to have a standardized framework where no unauthorized device (sensor or actuator) or even application is allowed to communicate. In a proprietary vendor locked-in scenario such fears and apprehensions are very difficult to be assuaged.

Data Sharing among Divergent Applications

In real world IoT/M2M Deployments, it is essential to have data sharing among divergent applications. This not only eliminates the need for exclusive and duplicate deployment of sensors, but also reduces a lot of burden on the network resources. Data sharing also enables efficient management of divergent Applications. However, in case of proprietary implementations, such sharing is controlled by the vendor.

Faster Development and rollout of new applications

Any application development which requires a painstakingly long development lifecycle is rarely acceptable to small players (including start-ups) as they would mean higher cost and unfavorable competitive environment for them. This favors only the large players as they are able to push dated applications and technologies to the market in a vendor locked-in scenario. Moreover, such solutions are never cost-effective and lack innovations.

Promote Innovations

For any technology area, the sustainability of a solution lies on its ability to withstand and accommodate change i.e. it should not curb innovations. A standardized practice which promotes innovations is the one which is going to survive the test of time and would witness the economies of scale.

Annexure C: Example of Data Sharing

A few years ago, when the connected car concept had just started, the premier car manufacturers like the BMW, Mercedes etc. used a lot of sensors in their vehicles. The data generated by these sensors were transported to their respective factories in a very proprietary manner. The communication was generally done using GSM network in international roaming. There was no provision to share this data and therefore other applications could not get the benefit of this huge data generated. Why data sharing is important and how the users get enormously benefitted can be understood by the following use case example:

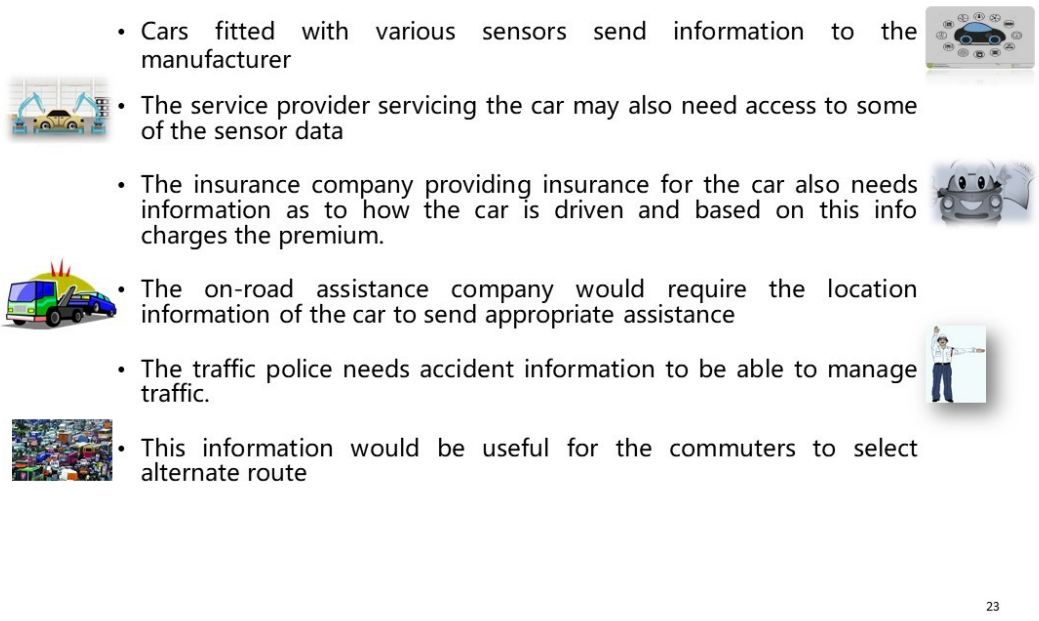


Figure 5: Data Sharing Example for Intelligent Transportation System

Nowadays majority of the cars are fitted with many types of sensors. These cars generally send information to their respective manufacturers, who in turn derive a lot of intelligence by analysing all this data to figure out how the parts of the car are functioning while being driven in a particular geography so that they can make modifications into his manufacturing process. These manufacturers can then build their cars suitable to that specific region or country. Unlike other countries, the Indian roads and traffic are very different, so the cars that are manufactured must be somewhat different than what is manufactured for Japan or Scandinavian countries.

A subset of this data thus generated by the same set of sensors can be very useful for the service provider who provides periodic service for the car(and this definitely is not the manufacturer) because he needs this information to cater to the client. So, the servicing partner is going to know as to what in your car is likely to fail, how your car is being driven, which inventory is depleting so that he can provide logistics information regarding that and he can replenish that part which

is likely to fail in your vehicle. The service provider can also give feedback that so many cars are behaving in a particular fashion, which need to be paid attention.

Another consumer of the data thus generated by the sensors in this car can be the insurance company , as the company insures user/driver by virtue of the driving pattern/skills.. The insurance premium thus charged can then be based on the driving skills and a safe driver can earn significant discount on the premium amount. This also would significantly reduce false claims.

Another beneficiary of the car's sensor data can be the on-road assistance company. Many of the car owners in the big cities subscribe to on-road assistance. The on-road assistance provider is only interested about knowing where a car has broken down and what part of the car has broken down, so that he can send the vehicle to user's comfort and rescue from them from distress. Even the traffic police will be immensely benefited by having access to this data because if a car has broken down during office hours in a busy city road, the traffic personnel will then have to send a towing vehicle straightaway or divert the traffic. Even the commuters need not depend on Google to know which route is congested.

Similarly, there can be many such application use cases where the data generated by the sensors if shared, can bring immense value. These applications become unviable if each of these applications are required to install their own exclusive set of sensors.

So, it becomes amply clear that the real benefit of the sensor data is obtained when divergent applications share it. This sharing has to be done in a secure manner with proper authentication, authorisation and accounting. Advocates of the proprietary siloed application providers may argue that the data can be shared from the business applications also. But that would require another management layer being created (figure below) which would extract data from all these applications. Not only it would be expensive, but also impracticable as this management layer would have to interface with such divergent proprietary implementations using non-standard APIs. This is far from being practicable. We must break these silos, if we really want to benefit out of IoT/M2M implementation.

Another major concern in today's communication systems and particularly IoT/M2M is Security. A security compromised IoT/M2M application may become a threat to human life as well due to the involvement of actuators (for taking actions). In view of this, it becomes necessary that this new IoT/M2M based ecosystem is well governed, secured and managed. However, this can only happen when we follow proven standards which are backed by well-defined policies. It is therefore a fact beyond doubt that we should have only authenticated and authorised, devices and applications and registered service providers in this domain so that these security concerns can be addressed.

Annexure D : About oneM2M

To provide a solution to these problems faced by the Cities across the Globe, eight (8) of the world's leading ICT standards development organizations, namely ARIB (Japan), ATIS (United States), CCSA (China), ETSI (Europe), TIA (USA), TSDSI (India), TTA (Korea) and TTC (Japan) came together to form a global partnership project named oneM2M®. The objective of oneM2M® is to develop technical specifications for a common M2M Service Layer that can be readily embedded within various hardware and software, and relied upon to connect authenticated and authorised IoT/M2M devices and applications in the field with the IoT/M2M application servers.

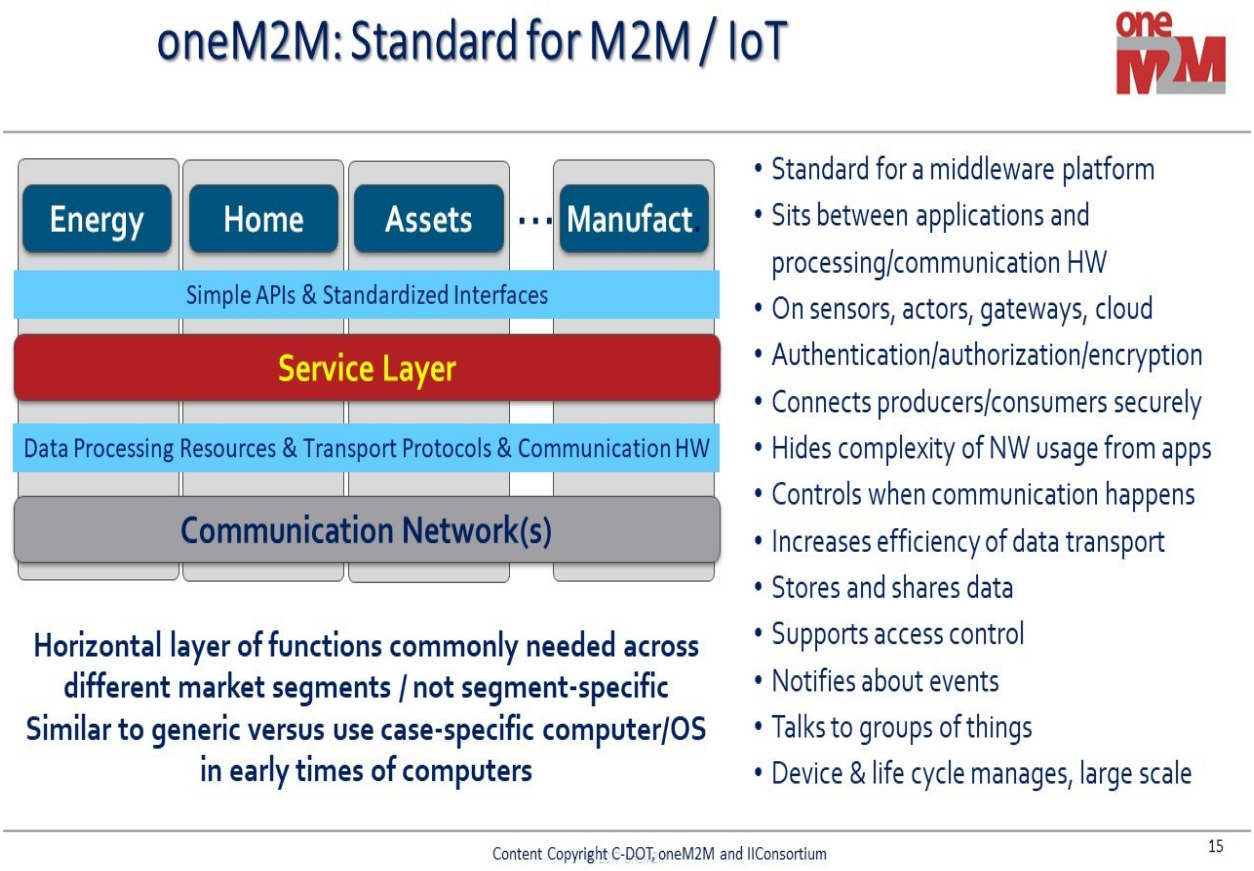


Figure 6: oneM2M Service Layer features

oneM2M has now been declared as the National Standard by Telecommunication Engineering Centre (TEC) and the same is also referred to in the BIS Standard (IS:18004 -IoT System part one – Reference Architecture). The oneM2M standards are also transposed by ITU-T under the Y.4500 series.

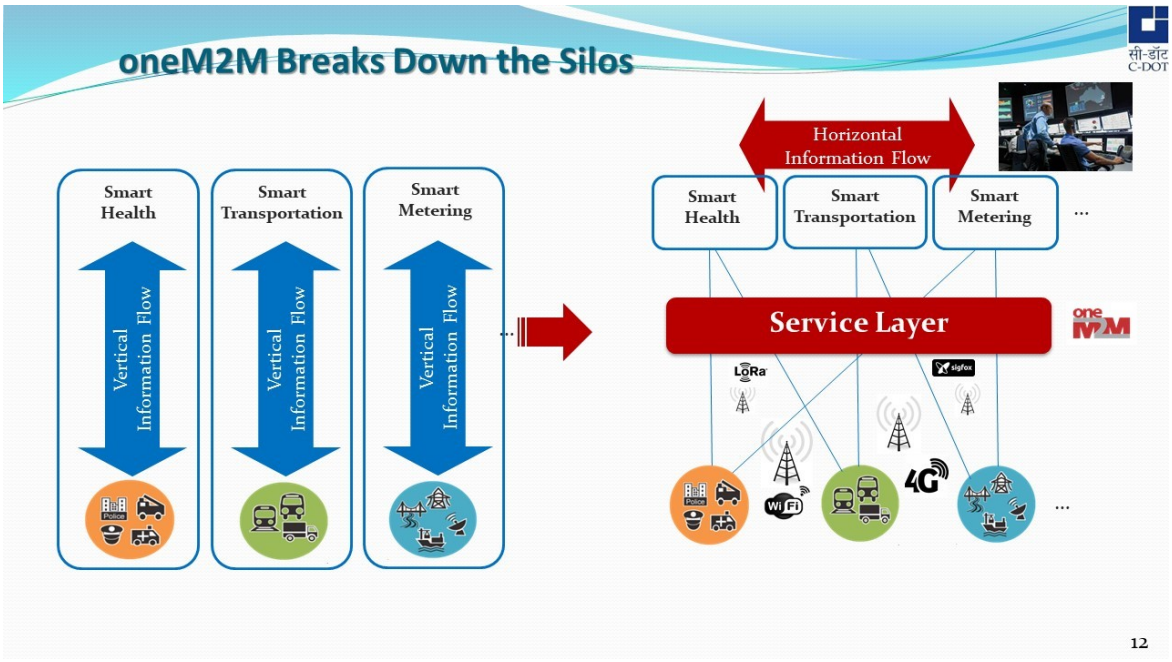


Figure 7: : Horizontal Information Flow using oneM2M Service Layer

The figure above shows how the common service layer breaks the siloes created by various domain specific implementations. The standardized common service layer enables horizontal information flow between various applications. The horizontal approach enables various divergent applications to share data among them without the need to be dependent on the various vertical centric application providers. The abstraction feature of the oneM2M standards, make it technology agnostic and as a result enables interoperability of devices, networks and applications. An illustration of deployment of Smart Street Light Solutions based on variety of network technologies using oneM2M based Common Service Layer platform is given below.

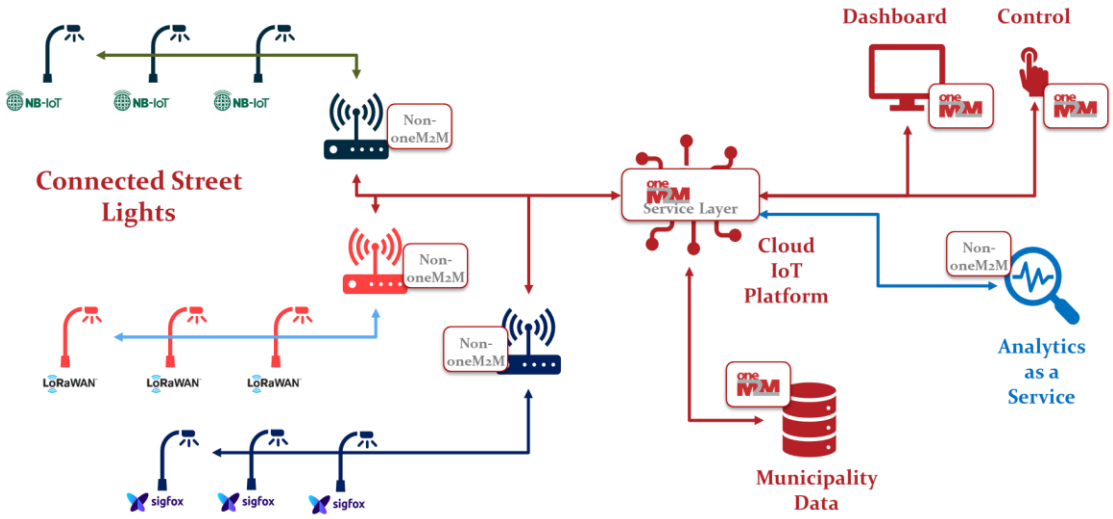


Figure 8: Interworking of various networking technology based Street Light Solutions using oneM2M Service Layer Platform

Annexure E : C-DOT Common Service Platform – CCSP

C-DOT Common Service Platform (CCSP), is the horizontal IoT/M2M platform based on oneM2M®. The USP of CCSP is in the Common Services Entity (CSE), which sits below the M2M application layer and above the transport layer. The CSE middleware breaks down silos by enabling applications to share a common services platform.

Another remarkable feature of the CCSP platform is that it is so flexible that it can accommodate a wide range of IoT/M2M communication protocols. Rather than attempting to pick technology winners, CCSP supports a wide range of established IP-based protocols for use between the Common Service Layer, network, and application layers.

CCSP allows use of Industry Standard ICT protocols by the devices and the gateways while providing 'Security as a Service' for M2M applications. It protects the M2M Service layer (authentication, authorization, confidentiality, integrity, privacy) and thus provides data integrity, data protection and privacy. With CCSP, cities can make more efficient use of existing networks and manage device and application proliferation in a much better way.

Why CCSP is important for India?

As most of the current IoT/M2M deployments including those in the Smart Cities have been proprietary platforms provided by large blue-chip companies, the large community of Indian IoT/M2M companies including the startups have not been able to contribute significantly in these endeavors despite being significantly innovative with their solutions.

CCSP, being an IoT/M2M platform based on oneM2M which is a National Standard, would be a game changer for these companies as they would now be able to create interoperable, standards compliant solutions around CCSP more rapidly than ever and can penetrate the Smart City Marketplace.

This would of great benefit to the Smart City Authorities as well who would now have far more open solutions to choose from without getting locked into proprietary platforms and solutions.

Annexure F : M2M enabled Smart Cities

IoT/M2M technologies have emerged as one of the most important important enablers in the present smart cities landscape, leading its paradigm to the big data scale. Smart Cities are one of the largest consumers of IoT/M2M applications and non-standardised, proprietary solutions have hindered the very fundamental requirement of these smart cities i.e., sustainability. Such implementations have caused interoperability problems due to the presence of many different IoT/M2M protocols, formats and frameworks and this aspect is enhanced by the fact that most of these smart city applications have been developed as vertical silos applications. By achieving a higher level of interoperability among devices, applications and services, the cities would benefit economically owing to reduction in costs for producing completely new and different deployments of the solutions. This would also allow backward compatibility through the exploitation of older systems as well as an incremental deployment and integration. The deployment of highly scalable IoT/M2M solutions can be much more cost-efficient by adopting a Standards Compliant Horizontal Architecture especially as more divergent applications and devices proliferate increasingly. Legacy implementations, through the development of adapters, can be brought onto the Standards Compliant Horizontal Platform without disruption.

In India, the Smart Cities Mission was launched by the Hon' Prime Minister on 25 June, 2015 with the objective to promote cities that provide core infrastructure, clean and sustainable environment and give a decent quality of life to citizens through the application of 'smart solutions'. Hundred cities were selected to be developed as Smart Cities through a two-stage competition. The Smart Cities Mission of the Government of India also backs the use of Internet of Things (IoT) /Machine to Machine (M2M) solutions for improving the quality of infrastructure and citizen services.

Annexure G : Industry Collaboration Application form

Indian organisations (including startups) working in the area of IoT/M2M and interested in collaborating with C-DOT for the development of oneM2M standards compliant applications may fill in the following form. Organisations found suitable would be granted access to C-DOT's oneM2M Standards Compliant IoT Platform-CCSP using which they can develop and test their oneM2M compliant Application. A Non-Disclosure Agreement would be signed with each Startup selected for this collaboration. Further details are available at https://coi.cdot.in

[The fields marked with * are mandatory]

1. Kindly provide a valid Email ID*

   .....

2. Name of the Organisation *

   .....

3. Year of Incorporation *

   Mark only one oval

   - 2010
   - 2011
   - 2012
   - 2013
   - 2014
   - 2015
   - 2016
   - 2017
   - 2018
   - 2019
   - 2020

4. Registered Office Address *

.....

5. Organisation's Website *

.....

6. Number of Employees *

Mark only one oval

- Less than 10
- 11 to 20
- 21 to 50
- More than 50 but less than 100
- More than 100

7. Did you know about oneM2M before? *

Mark only one oval

- Yes
- No

8. If the answer to the above question is yes, then please let us know whether you have developed any application based on oneM2M? *

Mark only one oval

- Yes
- No
- Not applicable

9. If the answer to the question above is yes, then please give brief description about the applications(s) along with the oneM2M release used for the application(s)

.....

10. Number of partners/owners of your Startup(in figures) *

.....

11. Name of the Primary Owner *

.....

12. Mobile Number of the Primary Owner *

.....

13. E-Mail Address of the Primary Owner *

.....

14. Name of the Secondary Owner

.....

15. Mobile Number of the Secondary Owner

.....

16. E-Mail Address of the Secondary Owner

.....

17. If there are more owners/partners, then kindly upload a separate excel sheet containing the name, mobile number and email address of all of them

File submitted:

18. Area of Work

Kindly furnish details about the work carried out in your startup in the following section

19. Name the domains/vertical industry you are catering to(Check all that apply)

- [ ] Asset Tracking
- [ ] Transport
- [ ] e-Health
- [ ] Environment
- [ ] Surveillance
- [ ] Solid Waste Management
- [ ] Smart Metering (Gas/Water)
- [ ] Safety and Security (including Fire detection, prevention and healthiness monitoring)
- [ ] Smart Home
- [ ] Active Assisted Living
- [ ] Any Other

20. Please upload PPT/PDF/DOCX file giving details about the application(s) developed

 Add file

21. Have you deployed your solution in the field ? *

- ( ) Yes
- ( ) No
- ( ) Deployment in progress

Give a brief writeup/presentation about your organisation: indicating your mission and vision, business model and how collaboration with C-DOT can be beneficial For the country as well as for each individual organisation. *

 Add file

A copy of your response will be emailed to the address you provided.