IoT-Center Pakistan

Initiative of Center of Information Technology(CIT)

Introduction of IoT Alliance Pakistan (IAP)

Introducing the Concept.

We are living in a time where the Internet of Things is truly ubiquitous in every ecosystem and industry. There are use cases embedded in all industries that utilize technology from home automation to manufacturing, healthcare and smart grid development. To date, IoT's most compelling use case has been in the industrial workplace, where whole sectors have been transformed by its ability to solve problems that have plagued traditional industries for centuries, from machine repairs and supply chain processing to worker shortages and waste management.

Similarly, today's farmer is most likely to rely on a smartphone than a pitchfork as they utilize IoT data to get the most accurate information about the weather, growing conditions, and their farm's soil quality – metrics previously unavailable or difficult to attain in real-time. At the same time, we see a whole new field of intersectional technologies rubbing shoulders with IoT: such as AI, Big Data, and machine learning.

All these trends are converging fast to provide most economical solutions for marginalized Communities specially in developing countries like Pakistan, but WE CAN ONLY BE BENIFITED if we bring in Place in Eco-Systems which provide equal playing ground to all Public and Private Sector Organizations to perform their respective functions within a framework mutually agreed after detailed discussions and considering Global Best Practices. In this Back Ground this was considered necessary by IoT-Center Pakistan to invite (Dated 21st July 2017) all relevant Stake holders to form IoT Alliance of Pakistan (IAP).

Some Facts about Internet of Things (IoTs)

a) The Internet of Things is a set of devices connected to the Internet interacting with each other and/or human actors, therefore, as a general matter standards and principles that are applicable to the Internet, are also applicable to the Internet of Things.
b) The Internet of Things is not just about objects, data collected and shared, and actions by those objects: it also has implications for people.
c) The Internet of Things, like the Internet, should be open, secure and accessible to all people.
d) To foster both innovation and user trust in the Internet of Things, like the Internet, a careful balance should be struck between regulation and space for innovation. This requires governments to hold back on regulation where possible, and industry to commit to self-regulation, where necessary, while recognizing that future useful/necessary applications as well as limitations cannot be determined yet, today, in full. Please note that current existing legislation that does not (yet) take IoT into account may affect the legal ability to deploy IoT products and services;
e) There are important benefits from the Internet of Things to deal with a wide range of societal challenges, ranging from social care, to agriculture, food chains, security and

environmental sustainability, and its development should thus be fostered and stimulated.

f) The Internet of Things is in its early phase and it is still evolving. Therefore, not all of the technical and the governance issues have been considered yet. Especially, the issues of security and privacy will need to be considered to ensure the justified trust in the Internet of Things environment.

g) The Internet of Things, needs investments in innovation and deployment in order to develop. Investors like to know that their investments will lead to products and services that are not countered by governments (illegal) or markets (seen as unsafe, unwanted, and unethical).

Need for a framework for IoT Good Practice

Good practice in IoT products, ecosystems and services require:

A.Meaningful Transparency to users: understandable and clear terms of use, including an overview what is tracked, and why, and how that information is used in IoT ecosystems and how it is shared with other companies or institutions and under what terms. Transparency also includes "usability" as it doesn't help to have options if you do not know how to use those, and "accountability" as it is important to know whom to address in case of wrong use or abuse;

B. User control of data produced by or associated with an application. This is necessary for multiple reasons, ranging from human rights to business and competition reasons. This user control may be reflected in various ways, through an ability to direct where data is sent or stored, whether the data is generated at all, be able to delete historic data, be in control of security settings for the data. For instance:

1. Ability to turn off individual tracking (and how this can be done) where and when possible, in the highest level of granularity as practically possible." All or nothing" does not always fit here, depending on the specific application. Another option would be allowing users to control access to their own tracking data via sufficient and useable means. In addition, it is clear that unless all people and objects around turn off tracking, "collateral tracking" may still happen;
2. Enable the user to protect their personal data with a technology of choice such as strong public key encryption;
3. Ensure user awareness of machine learning (and eventually possibly artificial intelligence) that may lead to change in behavior of IoT environments the user is confronted with;
4. Consider the ability to delete and export historic data: or at least makes sure that historic data are no longer related to individual accounts ("the right to be forgotten" in practice - and data can still be used for business process innovation etc.);

C. Security: IoT devices may have real, physical world connection and therefore, the implications of security may have physical or kinetic consequences. Therefore, the security of individual IoT devices, systems and the data related to the systems need to be secured adequately. An additional challenge raising from some IoT applications is the fact that the

devices and systems may be in use for a long time and the security requirements may change during that time.

D. Privacy: All stakeholders in the Internet value chain, which includes the Internet of Things, including governments and industry, including direct use and reuse of data, should comply with privacy and data protection norms and international law. In particular, any techniques to inspect or analyze Internet traffic shall be in accordance with global privacy and data protection obligations and subject to clear proactive legal protections.

Implementation and enforcement

An important element of loT Good Practice is its supporting mutual trust amongst all the components of loT ecosystems: human, devices, applications, existing institutions and business entities. Trust is boosted by a recognition of personal needs; by transparency in how things are organized-namely in a way that clearly shows that relevant measures have been taken to meet those needs-; and by accountability in ensuring that responsibilities are clear, and if someone responsible (person or organization) fails to live up to what is promise or required, they will be made accountable, thus assuming a principles based front end ("ethical") and harms based backend (accountable).

In order to ensure long term relevance of the products and services under development, it will be key to establish a clear framework for transparency and accountability, with respect for current legislation and pre-empting the evolution of the regulatory framework reflecting the changes in values and needs of the People of Pakistan.

Education & Awareness about IoTs

Related to loT, individuals should have the right to be educated or at least have access to information on which these individuals base their actions with loT - systems, - infrastructures and utilities. This education and proliferation of information needs to be done in a manner that is accessible to the non-expert and may benefit much from Open Educational Resources and prosumer knowledge base. It is important to ensure that all stakeholders are able to participate in the discussions and Form an alliance like IoT Alliance of Pakistan (IoT).

Some Suggested Do and Do Not's.

Based on my LONG EXPERIENCE in similar Situations where People with Versatile Domains and Roles & Responsibilities (Govt, Academia, Industry and Community) sit together to devise a Joint Strategy to make Policy, Strategy, Guide Lines, implementation laws to enable Departments, Organizations, Business Companies to follow Global Best Practices, I would like to suggest few Do & Do Nots for the considerations of the IoT Alliance Members.

Things To DO:-

1. Evaluate IoTs business values by engaging Govt org /Universities / IoT Companies / Vendors, Grassroot NGOs in Pakistan.
2. Holistically evaluate business opportunities and manage risk.
3. Prepare an Agreed ' **IoT Guide Lines** ' by relevant Stake Holders in Public / Private Sector.

4. Timely notify all stakeholders of anticipated usage in Different Sectors and vectors. (By IoT Knowledge Center to be developed jointly by all Public and private sector Stake holders) Engage business teams to implement some successful POC and Use Cases and help them to scale up under a sustained model.
5. Gather all stakeholders to ensure engagement and thorough planning specially Universities and IoT Knowledge Center for fast human resource development (IoT Engineers).
6. Look for points of integration with existing security and operational protections.
7. Examine and document information that is collected and transmitted by IoT devices to Analyze possible privacy impacts.
8. Discuss with relevant stakeholders when, how and with whom that information will be shared and under what circumstances.
9. Prepare a threat model under a IoT Security Policy / Balance risk and rewards.

Things Not to Do:-

1. Develop IoT policy / Strategy / Guide lines / laws in Isolation.
2. Let IoTs Vendors Deploy Solutions in Pakistan without consulting business or other public & Private stakeholders.
3. Disregard existing policy requirements, such as security and Privacy.
4. Ignore regulatory mandates.
5. Assume vendors (hardware, software, middleware or any other) have thought through your particular usage or security requirements.
6. Disregard device-specific attacks or vulnerabilities.
7. Discount privacy considerations or "hide" data that are collected/transmitted from end users.

Why we need IoT Partnerships

IoT-Center Pakistan is trying to engage IoT Companies in mutual partnerships because as a Global best Practices Organizations looking to implement IoT solutions are considering vendors that have a strong partnership strategy because **no one vendor can "do it all."** Strong partnerships are important for several reasons:

1. **Complexity of the IoT**. Many elements of technology, connectivity, and services must work together to achieve the outcomes desired. This span of capabilities requires vendors to develop alliances with other players in the IoT ecosystem.
2. **Industry-specific expertise**. Today, many IoT solutions are horizontally positioned. Many organizations need to have vertical capabilities to meet customer requirements that are specific to their industry focus. Horizontally focused vendors are looking for partners that intersect and augment their offering with industry-specific expertise.
3. **Holistic offering.** With one or many partners, a vendor has the ability to offer a more holistic solution set, thus helping address concerns specific to the organization.

What we need today.

1. A commonly agreed platform to respond to IoT Revolution (knocking our door).
2. Prepare IoT Guide Lines / Policy / Strategy / Laws / Regulations Immediately.
3. Bring in Place an Eco-System where all Stake holders can Help each other.

4. Rapid Human Resource Development in IoT Technologies.
5. NO Single Entity Can Do it !!!!!!

Suggestions for IoT Alliance of Pakistan.

Formation of FOUR Working Groups to submit their Recommendations by 5th December 2017 as Follows: -

- **IoTs Guide Lines. (Govt& All others)**
- **IoTs Virtual University. (Academia & Technology Partners)**
- **IoTs Market Place. (IoT Vendors Startups and SMS etc)**
- **IoTs for Communities. (NGOs,ISOC and E-Pakistan Teams)**
- **IoTs Security (Govt & All Stakeholders)**

Conclusion

The Internet of Things presents seemingly unlimited options for organizations (Govt, Universities, Vendors etc) looking to move toward digital transformation. In developing an IoT strategy, organizations need to work together to understand the complexity of IoT projects. It will be equally important for organizations to engage all Stake Holders in developing IoT Guide Lines, Policies, Strategy, Human Resource development so that vendors and organizations may work together to establish, proven, and strategic alliances to provide end-to-end solutions that address the industry-specific needs of the IoT investment in Pakistan.

Lets IoT Alliance of Pakistan (IAP) make it happen as a TEAM.

For Further Coordination Please Register at www.IoT-Center.org **and Contact :-**

Ammar Jaffri
CEO IOT-Center Pakistan
Ceo@IoT-center.pk
Ammar@Brain.net.pk
0300-8551479 / 051-2201520-21