ISSN:0975-9646

The Security SEAL : A Security Solution for SMART CITIES

Sri Harsha
Project Website : https://officialharsha.wixsite.com/amaravati (Temporary website)

INTRODUCTION

When a Smart City is all set to become the most technically advanced city in the world, its popularity invites treats and fears of terror attacks. We had been using National Security and it hasn't proven to be 100% safe and secure for mankind.

National Security is a concept which developed mainly in the United States after World War II, is the protection of the state and its citizens through a variety of means, including military might, economic power, diplomacy and power projection.

This concept can be improvised with our concept of THE SECURITY SEAL (SEA,EARTH,AIR,LAND) for any smart city.

BREAKDOWN

The Security SEAL is a new concept and project proposed to provide security to the newly built celestial capital of Andhra Pradesh, Amaravati. This Security system can be applied to other smart cities depending upon its performance and efficiency.

Security SEAL is divided into 3 phases:

1. BV < Before Visit >
2. DV < During Visit >
3. AV < After Visit >

Before Visit

Before visiting the celestial capital Amaravati, A Individual has to apply for visiting the state with his/her identification details approved by the government and answer a set of questions with the purpose of visit through a online government portal or website called ''AMARAVATI TRANSPORT PORTAL" (ATP).

The Data entry officers add/update the data of the applicant to a database which contains data of all the applicants a swell as of the data of the citizens .PostgreSQL does work fine for large datasets. The Data Scientist verify the complete profile and group the applicant as:

RED	< Potential Threat >
YELLOW	< Suspicious >
GREEN	< Clean >

Applicant has no idea of getting grouped into the safety groups. The Application is accepted or rejected depending upon the research done by the data scientist on a particular profile. Rejected applications are provided with valid reasons. Special medication and medical tests are also done in order to prevent bio-weapons entering the city.

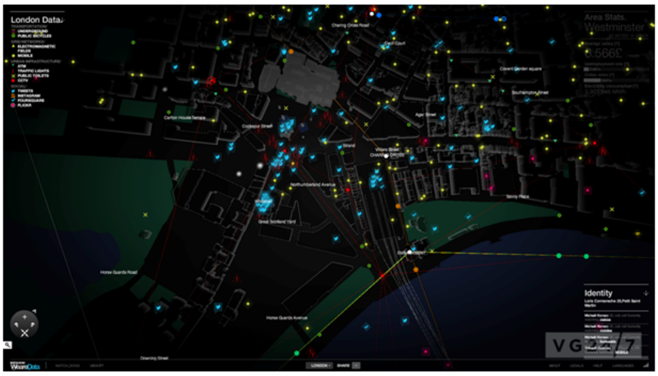
During Visit

After getting accepted to enter the city, the individual is provided with a digital band called iTrack which helps the SEAL security to trace the location and have the activities log of that particular individual in a database. The Citizens of Amaravati are provided with similar bands. The ''Amaravati Tourist Number" (ATN) and ''Amaravati Citizen Number" (ACN) are used as a property to categorize residents and non-residents of the city. The Smart city is going to controlled by CtOS (Central Operating System) a supercomputer that connects everyone and everything — including personal information, security cameras, and traffic lights.

The Band (iTrack) is predicted to look somewhat like this: (Pic of Cicret Smart Bracelet)

With this technology we can map the location of all the citizens. The Digital Band is mandatory for a individual to equip because without the digital bands, the individual cannot access to anything. For example – If he needs to use a bus or enter a store, he would require this band to get access. With the help of Iot (Internet of Things), the band transmits data to a data platform. Data platform is a gateway which keeps receiving a lot of data transmitted by different bands. The data is then sorted and stored in data lakes. All the necessary data and information are stored in Data warehouses. Fuse nodes along with cloud computing technology will also be incorporated for data transmission.

The Control Centre in Rio de Janeiro



Possible outcome of Human tracking System

This is a more advanced concept of human tracking over a large area using iTrack surveillance system. This means the location of a individual can be known at any point of time within the city.

The Internet of things

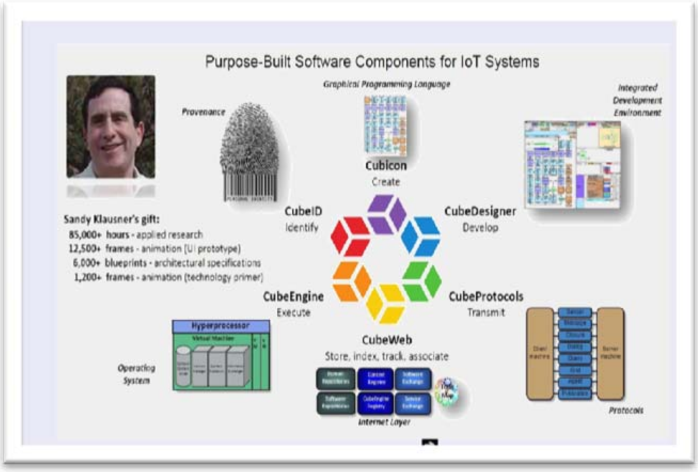
The Internet of things (stylized Internet of Things or IoT) is the internetworking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items—embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data. In 2013 the Global Standards Initiative on Internet of Things (IoT-GSI) defined the IoT as "the infrastructure of the information society." The IoT allows objects to be sensed and/or controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit in addition to reduced human intervention. When IoT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems, which also encompasses technologies such as smart grids, smart homes, intelligent transportation and smart cities. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure. Experts estimate that the IoT will consist of almost 50 billion objects by 2020.

IoT: Software is Critical and yet Challenged!

IoT Software Challenges :

- Scale, Distribution, Real-time, Security and Safety
- Modularity, Automation, and Reusability
- Vertical Experts not Programmers !
- Languages Do Not Capture Behavior
- Software for a Complex, Interacting Ecosystem with Data at the Core

We May Need a Clean Slate Approach to Software Development!!


Purpose-Built Software Components for IoT Systems
Sandy Klausner's gift:
85,000+ hours - applied research
12,500+ frames - animation (UI prototype)
6,000+ blueprints - architectural specifications
1,200+ frames - animation (technology primer)
Provenance
Graphical Programming Language
Cubicon
Create
Integrated Development Environment
CubeID
Identify
CubeDesigner
Develop
CubeEngine
Execute
CubeProtocols
Transmit
CubeWeb
Store, index, track, associate
Hyperprocessor
Virtual Machine
Operating System
Internet Layer
Protocols

Clean Slate IoT Software: Cubicon

Data Needs Help to Accomplish its Mission!!!

- Data needs to be extracted efficiently, in motion, cheaply, securely.
- Data needs to be "objectified and contextualized", as soon as possible, needs to be virtualized, securely stored, compressed, and analyzed hierarchically.
- Data needs to be moved, located, searched efficiently, cheaply, securely, around the infrastructure
- Rich Data awareness needs to be distributed from end-points to Clouds.

Data is Not the End of The Story!

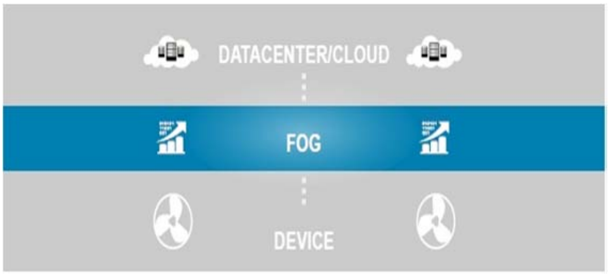
- Data needs to be used to Close the Control Loop!
- Good Analysis leads to Good Actions!
- The Convergence of IT and OT needs to deliver more efficient, scalable, effective Control of Systems

FPGAs Have a Great Role to Play in IoT!

- FPGA Technology can play a role in:
  - Supporting evolving standards in transport (e.g., Deterministic Ethernet (TSN)
  - Providing acceleration in data management and analytics (e.g., video analytics)
  - Acceleration in SDN applications at the Edge
  - Evolving security protocols
  - Storage evolving protocols
- FPGAs need to be made easier to program and more dynamic in their configuration
- FPGA main issue is COST!!!!!

Fog Computing

The fog extends the cloud to be closer to the things that produce and act on IoT data. These devices, called fog nodes, can be deployed anywhere with a network connection: on a factory floor, on top of a power pole, alongside a railway track, in a vehicle, or on an oil rig. Any device with computing, storage, and network connectivity can be a fog node. Examples include industrial controllers, switches, routers, embedded servers, and video surveillance cameras. IDC estimates that the amount of data analyzed on devices that are physically close to the Internet of Thing is approaching 40 percent.



There is good reason: analyzing IoT data close to where it is collected minimizes latency. It offloads gigabytes of network traffic from the core network, and it keeps sensitive data inside the network. Analyzing IoT data close to where it is collected minimizes latency. It offloads gigabytes of network traffic from the core network. And it keeps sensitive data inside the network.

How Does Fog Work?

Developers either port or write IoT applications for fog nodes at the network edge. The fog nodes closest to the network edge ingest the data from IoT devices. Then—and this is crucial—the fog IoT application directs different types of data to the optimal place for analysis, as shown in Table 1:

- The most time-sensitive data is analyzed on the fog node closest to the things generating the data. In a Cisco Smart Grid distribution network, for example, the most time-sensitive requirement is to verify that protection and control loops are operating properly. Therefore, the fog nodes closest to the grid sensors can look for signs of problems and then prevent them by sending control commands to actuators.
- Data that can wait seconds or minutes for action is passed along to an aggregation node for analysis and action. In the Smart Grid example, each substation might have its own aggregation node that reports the operational status of each downstream feeder and lateral.
- Data that is less time sensitive is sent to the cloud for historical analysis, big data analytics, and long-term storage (see sidebar). For example, each of thousands or hundreds of thousands of fog nodes might send periodic summaries of grid data to the cloud for historical analysis and storage.

Table 1. Fog Nodes Extend the Cloud to the Network Edge

	Fog Nodes Closest to IoT Devices	**Fog Aggregation Nodes**	**Cloud**
Response time	Milliseconds to subsecond	Seconds to minutes	Minutes, days, weeks
Application examples	M2M communication Haptics^2, ncluding telemedicine and training	Visualization Simple analytics	Big data analytics Graphical dashboards
How long IoT data is stored	Transient	Short duration: perhaps hours, days, or weeks	Months or years
Geographic coverage	Very local: for example, one city block	Wider	Global

What Happens in the Fog and the Cloud

Fog nodes:

- Receive feeds from IoT devices using any protocol, in real time
- Run IoT-enabled applications for real-time control and analytics, with millisecond response time
- Provide transient storage, often 1–2 hours
- Send periodic data summaries to the cloud

The cloud platform:

- Receives and aggregates data summaries from many fog nodes
- Performs analysis on the IoT data and data from other sources to gain business insight
- Can send new application rules to the fog nodes based on these insights

After Visit

This Phase is known as the development and feedback phase. Since we have the complete database of the city, we can improve and find more solutions.

For example, if we consider a tourist location like World famous Buddhist Stupa at Amaravati

We can survey the number of tourists visiting that location using the database. We can improve the economy by constructing more hotels and infrastructures that promote tourism in that particular area.

HACKING THE SMART CITY

The fact that all systems connected to the Internet appear vulnerable to cyber attacks is very worrying when considered in the context of smart cities. Unlike personal webcams, TVs and fridges, the technology of smart cities forms part of a complex and critical infrastructure which is used to calibrate and control a city. While governments and city authorities are generally slow to publicize attacks on their technological infrastructure, the Israeli government has acknowledged that essential services that run off sensors, such as water, electricity and banking, have been the target of numerous hacking attacks. For example, in 2013, the traffic management system for a main artery in the port city of Haifa, was hacked, causing major traffic problems that lasted for several hours. Such malicious hijacking of technology is inconvenient for citizens, costs the city financially and could also have fatal consequences. Last year, it was demonstrated that it was relatively easy to hack the traffic light system in New York City. By sending false signals regarding the traffic flow at particular junctions, the algorithm used to control the traffic light sequence could be outsmarted and fooled into thinking that a particular junction was busy and therefore adjust the green time of traffic lights in a particular direction.

City technology is built on legacy systems which have been incrementally updated as technology has changed. Security was often not considered in the original design and only added after. This makes such legacy systems more vulnerable for exploiting. For example, many of the traffic light coordination systems in cities date from the 1980s when the main security threat was physical interference. Another problem with the city technology is the underlying algorithms which can be purely reactive to the data they receive. If false data is supplied then the algorithm may produce undesirable consequences. While the discussion here has focused on sensors embedded in the city, other sources of data, such as social media are open to the same abuse. In March 2014, the twitter account of The Associated Press was hacked and a message reporting of an attack on President Barrack Obama was posted. This led to $136 billion being wiped of the NY stock exchange within seconds. This is an example of humans using bad data to make a bad decision. If the human cognition process is unable to interpret bad data, what hope do pre-programmed computer algorithms have?

As cities continue to roll out technologies aimed at enhancing the lives of citizens, they are moving towards data driven forms of governance both for long term and short term actions. Whatever type of sensor is collecting data, there is a danger that data can be biased, corrupt, played, contained errors or even be faked through hacking. It is therefore imperative for city officials to question the trustworthiness of data used in decision making. From a technical point of view, the data can be made safe by calibrating the sensors regularly and validating their readings against other sensors. From a security perspective, the hardware needs to be secured, maintained and updated to prevent malicious hacking of the device.

In other domains, such as the motor industry there is a move to transfer functions from the human operator to algorithms. For example, automatic braking, parking assistance, distance based cruise control and pedestrian detection are becoming mainstream in-car technologies in a slow move towards vehicles which drive themselves. It is likely that managing the city will follow the same pattern and incrementally the city will ‘drive’ itself and could ultimately be completely controlled by data-driven algorithms which react to a network of sensors. Although agencies such as the CIS give some advice to minimize the risk of Cyber Attacks on cities, it seems that hacking of the smart city infrastructure is inevitable. The reliance of cities on software and the risks associated with this strategy are well known (Dodge & Kitchin, 2004; Kitchin, 2014). The problem is compounded by the disappearance of the analogue alternative to smart city technologies (Townsend, 2013). This could lead to prolonged recovery from attacks and bugs due to the total reliance on technology to run cities. Cities therefore need to consider the security risks connected to deploying and using sensors to control a city and make decisions. It is also essential that control loops and contingency plans are in place to allow a city to function during a data outage just as contingency plans are made for handling the loss of other essential services such as power and water.

SUMMARY

In this chapter, we did a detailed study on the technical aspects of the security SEAL. We also discussed the advantages and possible drawbacks of SEAL. Next chapter, gives us an overall conclusion about the topic.

CONCLUSION

With this Concept, we will be able to prevent terror attacks like 9/11 from occurring again in the future. We understand, advance and outperform any kind of threat to the safety and security of the nation. Depending upon the efficiency of the project, it can be developed for any country. Decisions like issuing executive orders and temporarily barring refugees from seven Muslim-majority countries entering the US won’t actually help the situation. This creates a lot of distress, criticism and riots within and outside the country. The proposed project can actually be a possible solution to all such problems.

REFERENCES

[1] IoT: The Convergence of Information Technologies and Operations Technologies Flavio Bonomi (presented by Gordon Brebner, Xilinx)

[2] Human tracking System using RFID ,Department of IT,MEFGI

[3] Fog Computing and the Internet of Things, CISCO

[4] Smart and Digital City: A Systematic Literature Review Annalisa Cocchia

[5] Dodge, M., & Kitchin, R. (2004). Flying through code/space: The real virtuality of air travel. Environment and Planning A, 36(2), 195–211.

[6] Townsend, A. (2013). Smart cities: Big data, civic hackers, and the quest for a new utopia. New York: W.W. Norton & Co.

[7] Kitchin R. (2014). The real-time city? Big data and smart urbanism. GeoJournal, 79(1), 1–14.

[8] DRAFT PE RSPEC TIVEPL AN – 2050 For Andra Pradesh Capital Region

[9] E-Government Interoperability : Interaction of Policy, Management, and Technology Dimensions, Theresa A. Pardo, Taewoo Nam and G. Brian Burke, Social Science Computer Review 2012 30: 7 originally published online 12 January 2011

[10] Memory in Motion. Archives Technology and the social, EDITED BY INA BLOM,TROND LUNDEMO AND EIVIND RØSSAAK

[11] Do they read your research? An investigation of practitioners’ use of IT outsourcing and cloud sourcing research, Australasian Conference on Information Systems 2016, Wollongong

[12] Smarter Cities Thought Leadership White Paper, IBM

[13] Cognitive Government Enabling the data-driven economy in the cognitive era, IBM

[14] Fooling the ‘SMART CITY’ ,Denis Makrushin, Vladimir Dashchenko, Kaspersky Lab

[15] Cisco Smart Connected Safety and Security Solution, CISCO

[16] (Ab)using Smart Cities, The dark age of modern mobility, Matteo Beccaro, Founder & CTO at Opposing Force, matteo.beccaro@opposingforce.it, Matteo Collura, Researcher at Politecnico di Torino, eagle1753@onenetbeyond.org

[17] ICT-enabled Administration of Commercial Taxes – A Case Study of Andhra Pradesh ,Dr. Sridhar Raj ,Dr. Sita Vanka ,Mr. Suresh Chanda

[18] e-Governance Initiative at Andhra Pradesh Transport Department: A Case of Process Reengineering of Driving Licence Process ,Dr. A K Rao

[19] Internet Of Things at Home, Ashwin Agarwal / Pivotal Inc. ,Bala Thumma / Synopsys Inc. ,Koushik Rajan / Yahoo Inc., Murali Repakula / Juniper Networks, Inc, Sarvesh Bhardwaj / Mentor Graphics, Inc.

[20] Fog Computing and Its Role in the Internet of Things,Flavio Bonomi, Rodolfo Milito, Jiang Zhu, Sateesh Addepalli, Cisco Systems Inc., 170 W Tasman Dr. San Jose, CA 95134, USA ,{flavio, romilito, jiangzhu, sateeshk}@cisco.com

[21] Internet of Things: Wireless Sensor Networks, Wireless Sensor Networks project team, in the IEC Market Strategy Board

[22] Understanding Internet of things, Connected Living, GSMA

[23]