Features and Potential Security Challenges for IoT Enabled Devices in Smart City Environment

Dr. Gasim Alandjani
CSE-ICT Department
Yanbu University College
Yanbu Alsinayah, Kingdom of Saudi Arabia

Abstract—**Introduction of Internet of Things in our lives have brought drastic changes in the social norms, working habits, ways of completing tasks and planning for future. Data about our interactions with everyday objects can be effectively transmitted to their destinations with many communicating tags that also often provide specific location information. The risk of potential eavesdropping is always a major concern of data owners. Since Internet of Things is primarily responsible for carrying data of smart objects which are mostly connected over wireless technologies, securing of information carried by these wireless links to safeguard the private information is of utmost importance. Cryptographic techniques to cypher data carried by the IoT networks is one possibility which is not feasible due to the lack of sufficient computing resources at the sensor end of IoT devices. In this paper, we discuss various security issues that haunt the secure IoT deployments and propose a layered solution model that prevents breach of security during transmission of data.**

Keywords—IoT; privacy; smart city; smart society; actuators; sensors; industrial 4.0;5G

I. Introduction

Technology is taking us to the next level for providing end users with state of the art services by using latest cutting-edge technologies. As far as security is concerned for all these latest technology we can take example of Internet which is still not secure, so same is the case with other technologies and eventually there is no expectations that IoT will be secure. However, with the passage of time security is constantly evolving to meet new challenges and also addressing the old ones that we've faced in past, and we'll see them again, with IoT and succeeding associated technologies.

Leading companies have stopped development for old technologies and shifted development for latest cutting-edge technologies, recent example is Intel who drops plans to develop spectre microcode for ancient chips.

New manufacturing processes generally result in faster and more efficient processors, and time is not far when this gap will close, thus providing developers with enough processing power in these devices to implement enhanced and better security features.

According to research firms International Data Corporation (IDC) and Gartner, IoT will grow to technology to such advance level that which will change layout and processing requirements which are available in current format of data centers. Gartner predicts by 2020 IoT market will have 26 billion devices will have IoT enabled sensors, which eventually will be creating huge opportunities for for hardware manufacturers, data centers users, and developers. IDC also expects huge investment in IoT industry with "billions of devices and trillions of dollars" by the end of the decade and resulting with the following potential challenges.

- Enterprise: Security issues could pose safety risks.
- Security: Increased automation and digitization creates new security apprehensions.
- Data: Tons of data will be generated, both for big data and personal data.
- Consumer Privacy: Potential of privacy breaches.
- Data Centre Network: WAN links are optimized for human interface applications, IoT is expected to dramatically change patterns by transmitting data automatically
- Server Technologies: More investment in servers will be necessary.
- Storage Management: Industry needs to figure out a cost-effective way to deal with tons of data generated by these IoT enabled sensors.

As technology is getting smarter there is great increase in popularity of tinny technological gadgets including Smart wristbands, toasters and dog collars which aren't a huge concern from a security perspective, due to low cost and there is lack of processing power in these devices which is another security problem, as most advanced encryption techniques simply wouldn't work very well, on the other hand if more processing and storage capacity is added to these devices which will eventually increase their cost and will throw than out of the competition of these popular devices. In a Survey HP reviled that 70% of IoT devices are vulnerable to attackers.

Here is a list of points to consider that can help in improving security.

- Security emphasis from day first
- Lifecycle, future-proofing, updates
- Consideration for Access control and device authentication
- Never underestimate power of hackers

- Well Prepare for possible security weak points and their solutions.

Based on usage, network location and processing power of IoT devices the level of threat varies from device to device and there are uncountable concerns to consider while using them for domestic purpose end users should have sufficient knowledge about all these threats before they start using these devices at homes and offices for personal use.

Users should be ready for potential security breaches. As they are inevitable, it can happen to you or someone else. Make sure that you should always have a solution for any possible security breach for maximum security of data and interpreting compromised data useless without breaking your IoT infrastructure(most the time It infrastructure in offices is and will be more secure as compared to normal users who will be using these devices for personal use at their homes.

If they are interested in expanding services through the IoT then they must keep consumer choice and preference while deciding which capabilities they would deliver on a smartphone versus a smart watch. Similarly, a Mobile App Development Service Provider should use the same lens while developing applications for those connected devices.

While talking to user end services in smart city, which is offering a vast range of device automation and management at user side. The major security issues in IOT field are confidentiality, authentication, access control, trust, mobile security, privacy, policy enforcement and secure middleware.

II. Related Work

Security in IOT is very interesting topic these days. Many projects are started in this context. One of the projects is Butler which is European Union FP7 projects. It provides secure context-aware and location aware services to assist smart home, city, hospitals and business domains. [1] describes about Iot applications and their interaction with each other based on different nature of hardware interfaces different devices are not able to communicate properly so is the case with different types of applications which have been designed but still there are some missing dots that need to be filled to get maximum from these IoT based application which have been used to provide different services.[2] describes the Hydra project develops middleware for network embedded systems based on service oriented architecture. This project deals with security issues and trust issues among distributed components of middleware. The role of middleware is to incorporate among heterogeneous devices using different technologies. [3] Describes basic principles with methodology of experiment which will be bridging social network interactions and sensor measurements. Its aim is to exploit the smartSantander for sensor measurement and communication to the public. And also to analyze and summarized sensor reporting and development of collective aware applications. [4] Describes uTRUSTit project which is usable trust in Internet of things. It offers the trust feedback toolkit in order to enhance user security. [5] Describes for consideration of a particular city as smarter one based on different practices. It has used a set of multidimensional components as a core factor for smart city and successful delivery of its services. It also offers strategic principles aligning to technology, people, and institutions of smart city and it further goes to show human learnings based on these facts. [6, 7] describe that most studies on practices of smart city address issues of technological infrastructure and associated enabling technologies. The focus on state of the art infrastructure will help technology, accessibility and availability of systems. [8] describes the iCore project which is large management system for IOT in ecosystem. It consists of following components VO virtual objects, composite virtual objects and real world objects. In USA there are also many IOT based projects. One of the projects is proposed by DARPA which is High Assurance Cyber Military System (HACMS), it assures that military vehicles, equipment and drones cannot be hacked from outside. Roseline is another project which is issued by NSF. Its work is to enhance the robustness in cyber-physical systems. Furthermore NSF projects are: XIA-NP (Development-Driven Evaluation and Evolution of the expressive Internet Architecture) which describes the diversity in network models, NDN-NP(Named Data Networking-Next Phase addresses the technical challenges like routing, scalability, fast forwarding, trust models and privacy. NEBULA provides architecture for cloud computing, and Mobility next Phase describes general mobile delay tolerant. These projects will explore novel network architecture and protocols. Further projects are included by National Basic Research Program focuses on the Security Protection among different entities of IOT.FIRE (Future Internet Research and Experimentation) is a project of Europe, China and Korea which is realization of different IOT technologies in different areas. EU-JAPAN cooperate for developing global standards and seamless communication.[9] describe a cloud model for provision of efficient services to the end users without compromising their personal security which using cloud any community cloud, it further describe different available solutions based on different types of clouds e.g public cloud, private cloud and community cloud. [10] describes a triple-helix model which enable to study the knowledge base of an urban economy for local community support regarding evolution of key components of innovation system, it further claims that cities can be considered as the intellectual capital of universities, the wealth creation for industries and democratic government for civil society interaction of these three densities generate dynamic spaces where knowledge can be used for bootstrap as technology for regional systems.[11] describes the conceptual scene for city e-governance, with a major focus on creation of cooperative digital environments to enable local competitiveness and prosperity through knowledge networks and partnerships, it further showed results of a very detailed survey study in which was conducted in twelve European cities. [12]describes smart infrastructure framework development supported by survey regarding accuracy for position of any devices which have been used for providing services to the inhabitants of smart society, it also discusses main advantages of proposed architecture with measureable and non-measureable benefits. [13] describes a smart innovation ecosystem characteristics which clarify the assembly of all smart city concepts into green , open, instrumented, integrated and intelligent layers which further compose a planning frame work which is called smart city reference model based on different shapes and sizes of cities. This model can be used to for smart policy paradigms and encirclement the green, broadband and urban economies. [14] Explains the industrial 4.0 where human will be replaced by AI based robots which can be controlled by augmented reality based on needs and typical routine requirements of work flow and in case of emergency to control the delicate processes and critical situations. [15] Highlights the issues that can be a reason in increase of multidimensional challenges for both (city residents and administration) entities of smart cities and further proposed a conceptual framework of cloud based architecture context aware smart services for inhabitants of smart cities. [16] its discusses about some standard navigation system which help to create a navigation model which can be used to find location of service providing devices installed on different locations of smart city. [17] described about future trends which will be going to create a community where classes will be defined based on community services for different classes and it will further create an environment of a jail-less community where there is be no conventional jail for criminals rather they will be deprived of some services and they have to inform local police before leaving premises of smart city.

There is enormous pressure on the city management to provide sustainable services and facilities to the growing cities paving the way to launch smart city initiatives by the government, public and private sector. IoT has also gained importance in smart city development. IoT facilitate people and things to connect with each other at anytime, anyplace, with anyone by using any network to access their required services. Smart city concept revolves around six fundamentals namely, smart people, smart governance, smart economy, smart mobility, smart living and smart environment. Smart City and IoT are evolving together to achieve the same goals. IoT heavily relies on cloud services for data consolidation, big data analytics, reporting and web front-end etc. Everything as a service (XaaS) is the concept offered by cloud to offer different levels of services as per the requirements of the end users or devices. The basic idea behind cloud computing and storage is to concentrate resources such as hardware and software into geographically diverse locations and offer those resources as service to large number of consumers who are located in many different geographical locations. There are three well defined levels of cloud services i.e. Platform-as-a-Service (PaaS), Infrastructure-as-a-Service (IaaS), and Software-as-a-Service (SaaS). Based on these models sensing as a Service model is designed to address solutions for IoT and challenges in Smart City. It consists of four Conceptual Layers as mentioned subsequently:

III. Major Security Challenges

There a numerous security challenges for IoT devices with current available infrastructure as of now and providing connectivity in smart city environment.

A. Technical Sophistication Gaps

A multifaceted system of connected devices opens many new attack vectors, even at individual level if each device is secure while not connected to network. Since a system's most vulnerable point decides its overall security level, a comprehensive, end-to-end approach is required to secure it. Which is very difficult to develop.

B. Absence or Immaturity of Standards

The IoT lacks well-established predominant standards [17] that describe about different components of technology should interact. Some segments, such as industrials, still rely on a small set of proprietary, incompatible technology standards issued by the major players, as they have done for many years. In other segments, such as automotive or smart buildings, standards are basic. Development of end-to-end security solutions in absence of common standards will be difficult task for IoT device manufacturers.

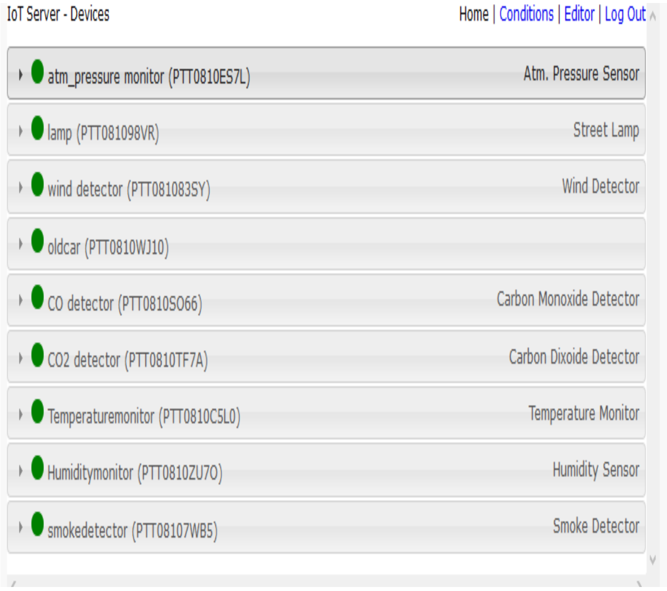
C. Consideration of IoT as Commodity

With all new productive gadgets of IoT majority of customers still consider it more as commodity rather considering it a mature product that's the main reason they don't think to go for security of these devices.

D. Challenges for Manufacturers

Most of the semiconductor manufacturing companies are currently struggling a lot to embed security features during manufacture process as it result in high cost and difficult to meet market cost effective demands. One side role f IoT in smart buildings is expected to increase by 40%, On the other hand IoT security breaches are rising in residential applications. This security trend may vary at user end based on their usage behavior e.g. some users might update firmware continuously on the other side some might not be updating them which will eventually become a potential security risk for these devices.

There is a great need to propose a sensor network model which follow the layered approach and get data in a systematic way from different sensors according to requirement for communication.



IoT Server - Devices

● atm_pressure monitor (PTT0810ES7L)	Atm. Pressure Sensor
● lamp (PTT081098VR)	Street Lamp
● wind detector (PTT081083SY)	Wind Detector
● oldcar (PTT0810WJ10)	
● CO detector (PTT0810SO66)	Carbon Monoxide Detector
● CO2 detector (PTT0810TF7A)	Carbon Dixoide Detector
● Temperaturemonitor (PTT0810C5L0)	Temperature Monitor
● Humiditymonitor (PTT0810ZU7O)	Humidity Sensor
● smokedetector (PTT08107WB5)	Smoke Detector

Fig. 1. Data Collection through Different Sensors.

This data can be collected by using different low computing devices including smart phones. Below figures are depicting different types of data collected by different sensors and then further plotted them against different values which smart city users will be using collecting data of smart environment to show it from different aspects.

Fig. 1 is showing data of different sensors which we have calibrated by use of Cisco Packet Tracer software, where we can add different sensors and read output for different values in any given scenario before its physical deployment.

Fig. 2 is showing different levels of atmospheric pressure at different intervals of time, these values have been taken in normal situation, in case if some unauthorized person manage to get access to this system with intention to alter it for some specific goals results could catastrophic as people might be relying on output values provided by these sensors. In case they get some wrong results at some critical time which might generate great loss.

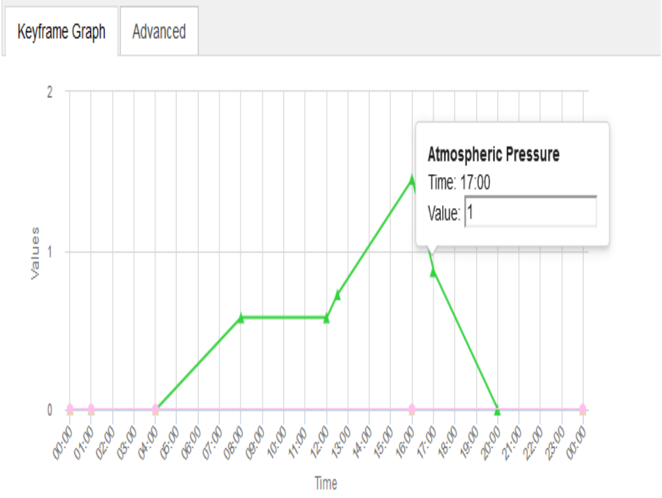


Fig. 2. Atmospheric Pressure.

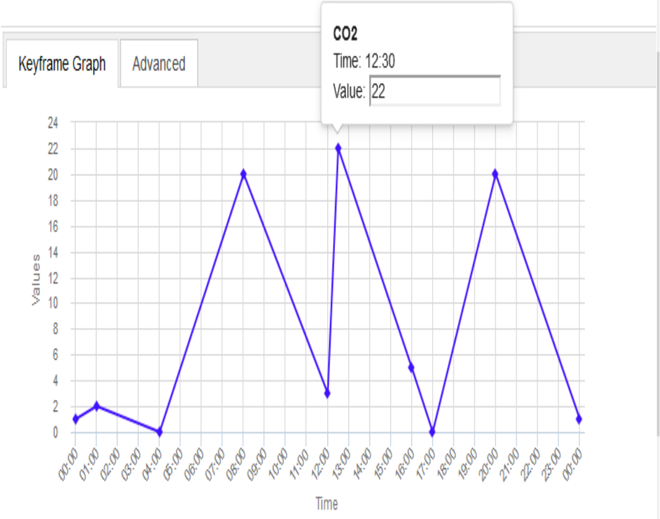


Fig. 3. Carbon Dioxide Levels.

Fig. 3 is showing different levels of Carbon Dioxide at different intervals of time, these values have been taken in normal situation, in case if some unauthorized person manage to get access to this system with intention to alter it for some specific goals results could catastrophic as people might be relying on output values provided by these sensors. In case they get some wrong results at some critical time which might generate great loss if there is extra ordinary increase in CO2.

Fig. 4 is showing different levels of ambient temperature variation at different intervals of time throughout the whole day, these values have been taken in normal situation, in case if some unauthorized person manage to get access to this system with intention to alter it for some specific goals results could catastrophic as people might be relying on output values provided by these sensors. In case they get some wrong results at some critical time which might generate great loss if there is extra ordinary change in environmental temperature and it might further make is critical for industry especial in the presence of industrial 4.0 if it goes unnoticed due to fake readings presented through any compromised IoT monitoring system.

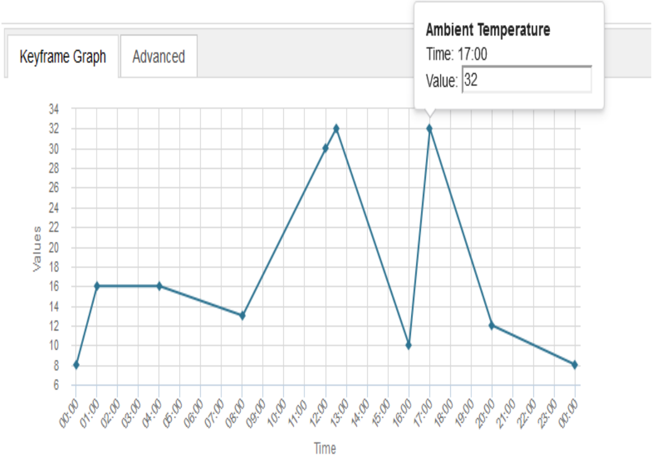


Fig. 4. Ambient Temperature Variations throughout a Day.

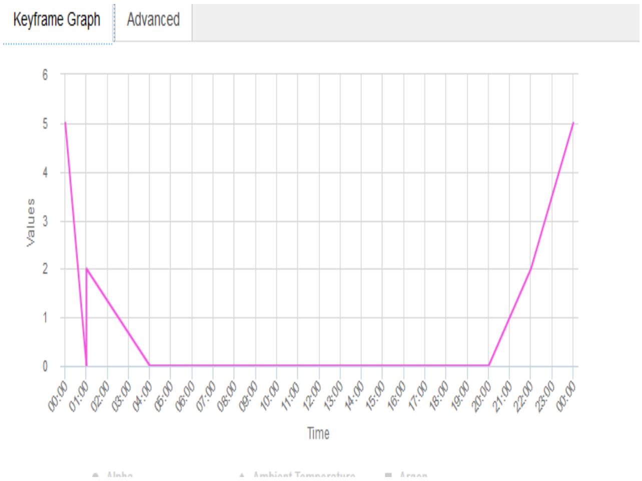


Fig. 5. Humidity Level throughout a Day.

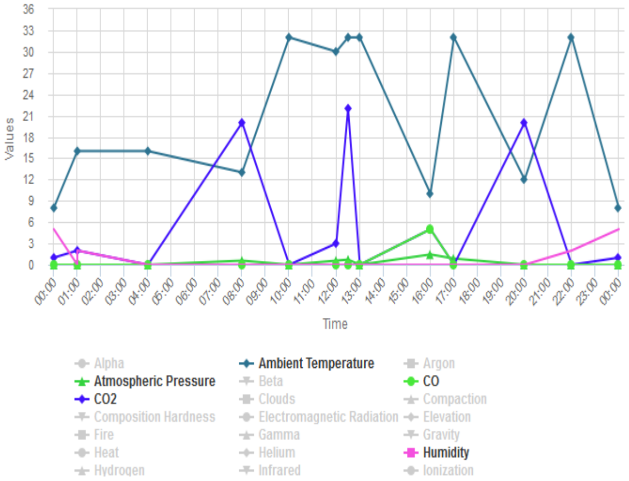


Fig. 6. Sensors Data Graphical View.

Fig. 5 is showing different levels of humidity at different intervals of time, these values have been taken in normal situation, in case if some unauthorized person manage to get access to this system with intention to alter it for some specific goals results could catastrophic as people might be relying on output values provided by these sensors. In case they get some wrong results at some critical time which might generate great loss if there is some extra ordinary change in humidity.

Putting all these together, Fig. 6 is showing all data in a single graph for values of all these sensors. Showing them at a single graph help to read understand overall data trends for different sensors. In case they get some wrong results about any of the above sensors at some critical time which might generate great loss if there is extra ordinary change in environmental temperature, CO2, Humidity, atmospheric pressure and humidity level. it might further make is critical for industry especial in the presence of industrial 4.0 if it goes unnoticed due to fake readings presented through any compromised IoT monitoring system.

IV. IoT Security Services

Following services are used by IoT devices in smart city environment sharing data through sensors.

A. *Authentication*

For authentication and confidentiality they have discussed work proposed by various researchers. One of the proposed method is custom encapsulation mechanism which includes encryption, signature and authentication. The two way security authentication scheme is also very popular. It uses Datagram Transport Layer Security (DTLS) protocol which is present between transport and application layers. It uses RSA which is designed for IPv6 low power wireless personal area network (6loWPAN). It provides integrity, confidentiality and authenticity with affordable energy, end-to-end latency and memory overhead. The key management system has four major categories key pool framework, mathematical framework, negotiation framework and public key framework. Some of the KMS protocols are not suitable for IOT ,for example key pool framework has connectivity issue, mathematical evaluation needs optimization to construct data structure, however some of the KMS are effective like Blom and polynomial schema whose computational overhead is low and use public key infrastructure (PKI). A transmission model which uses signature-encapsulation schemes and provides anonymity, attack-resistance and trustworthiness. This model utilizes object naming service (ONS) queries. Root ONS authenticates queries by local ONS via trusted authentication server (TAS) and prevents illegal ONS. Remote information server of things (R-TIS) wraps the information in encryption layer with the public key of routing node. The information is routed at every node until the local information server of things (L-TIS) receives plain text. However this method is weak in attack-resistance. Although above methods provide better security in terms of confidentiality and authentication but some questions are really answerable i.e. at which layer we should apply security mechanism, how to handle keys, which key distribution method will be useful, can we use previous authentication mechanism and how to apply end-to-end integrity to prevent malicious attacks. Some of the recent work to address such questions is authentication mechanism for IOT using lightweight encryption using XOR manipulation for anti-counterfeiting and privacy protection, for WSN user authentication and key agreement between users and remote sensors and another lightweight encryption mechanism called elliptic curve cryptography (ECC) for authentication and attribute based access control.

B. *Access Control*

Access means how different resources are provided to different users. Two terms are frequently used; data holders which are users and things while data collectors are sensors and service providers. In IOT data streams have to be processed and many queries are generated so enough data manipulation is needed. Every node is given a limited computational, storage capacity and single key. Other keys are manipulated so storage capacity is saved. The authentication system for emergency cases e.g. in case of accidents availability, name and location must be provided. Nile security architecture is also very popular which process data streams by frequent queries using cipher encryption and decryption keys. The authentication process for the outsourced data (in cloud computing). It involves authentication from the source and process queries for clients so data from authenticated sources are processed and clients get the right.

C. *Trust*

Trust concept is related to security and access control. The researchers have described how devices are heterogeneous, different users share friendship and belong to different community so malicious attacks are common. Self-promoting, good mouthing and bad mouthing are trust related attacks. The trust management protocol. It is distributed, encounter-based and activity based.it means that when two devices communicate with each other they perform trust based evaluation with each other. The evaluation parameters are honesty, cooperativeness and community interest. The reputation based trust mechanism for the IoT nodes to prevent malicious node and ensure communication for the trusted nodes only. They proposed a subjective model for P2P devices, in this model each node computes the trustworthiness of the neighbor node and ensures communication with only trustworthy node. The secure ad-hoc networks it provides peer to peer communication and communities to surf web. It involves following parameters to analyze; physical proximity, fulfillment, consistency of answers, hierarchy on trusted chains, similar properties, common goals, availability and interactions. The phenomenon of fuzzy approach to trust based access control (FBTAC). Trust scores are calculated by factors like experience, knowledge and recommendations. It consists of three layers device, request and access. Device layer consists of all devices, request layer consists of all the recommendations and fuzzy results and access layer involves decision making. This fuzzy approach provides flexibility and scalability. It is easier in utility based decision making. Fuzzy approach based upon three layers; sensor, core and application layers. Sensor layer consist of physical devices like sensors and RFID, the core layer consist of access network and internet. Application layer consists of distributed networks (e.g. P2P, grid, cloud computing). Evaluation of trust management by fuzzy set theory and semantic based language on layered approach and layer attributes are history, risk and efficiency. In this model user can access to the IOT devices only if the security credentials are satisfied. A trust model by utilizing the location, identity and authentication history. There are three trust regions based on trust levels:

i. High trust level
ii. Medium trust level
iii. Low trust level

In high region of trust no authentication is required only VID is used. In medium region users offer their PIN to login, in low region of trust different authentications are required like face identification, fingerprints and iris scan. The trustworthiness of nodes by their past behavior. It involves following steps;

i. Gathering of information about the trustworthiness of neighboring nodes.
ii. Set up collaborative service with neighboring nodes.
iii. Learn about the previous operation and update.
iv. Assign a quality recommendation score to each node.

Attack resistant model is proposed by researchers for distributed approach. It provides trust in self-organized nodes and attack resistance in distributed nodes. The WSN nodes and provides identity based network to the devices. It prevents attacks from the malicious nodes. The identity management systems for nodes which move from host to host so they need location and identification to separate from host addressing. Following techniques have been used, to achieve trust, so for social networking, fuzzy approach, identity based networking and cooperative approach. Following issues are still open in Trust management.

i. Introduction of semantic based language for the negotiation of trust.
ii. Proper identity management system.
iii. Development of trust management system for data stream control.

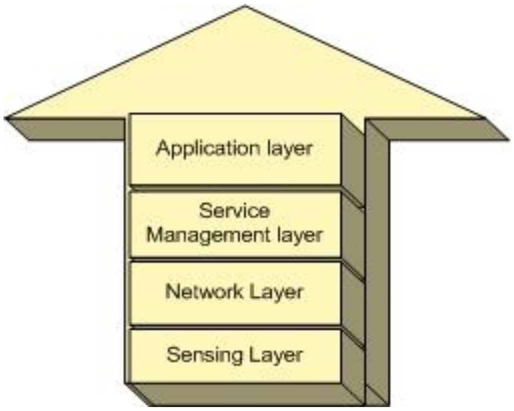


Fig. 7. Layered Architecture of IoT.

D. *Mobile Security in IOT*

Mobile nodes move from one cluster to another so rapid identification, authentication and privacy protection is required. The ad-hoc network protocol when nodes move from one cluster to other. It uses request messages and answer message for identification, authentication and privacy protection. This process has less overhead, more security and protection. HIMALIS (Heterogeneity Inclusion and Mobility Adaptation through Locator ID separator).it proposes secure and scalable mobility management. It provides secure inter domain authentication, secure location update and binding transfer for mobility process. RFID system based upon Electronic Product Code (EPC). It explains the mobile threats of RFID nodes. It guarantees security and efficiency. The security of tag and readers are also very important aspects. It also explains tag corruption, reader corruption, multiple readers and mutual key exchange protocol. The location security issues in mobile nodes. It pays attention to special location issues in android, iPhone and windows network platform. the secure handshake between mobile nodes in intelligent system is also a prime concern. Mobile node verifies the legitimate sensor node over an insecure channel via negotiation of handshake protocol. The mobile solution for healthcare services. It provides security and privacy mechanism for the security of the patients. The RFID tag identification and IOT infrastructure is combined. Efficient and secure mobile intrusion detection system for business applications using human centric computing is in placee. The mobile information collection through IOT gateway via smart devices. Quantum Lifecycle Management System messaging standard to provide two way communications between firewalls is also very interesting idea for security. Mobile Sensor Data Processing Engine (MOSDEN) is another technique. It collects and processes sensor data without programming efforts .it uses plug-in based IOT platforms for mobile devices. Other techniques are discussed by different researchers like video dissemination for IOT devices, interaction of smart things via Bluetooth and use NFC via mobile devices via Web of Things.

1) Proposed Solutions: As there is no complete solution related to internet security, same is the case with IoT up till now there is no single major solution regarding security and privacy of IoT devices, infect IoT devices are more prone to hackers and attackers due to the fact that IoT communication is primarily a sensor based communication which further make it more independent when devices start communicating to other devices without waiting for permission from human or without interference of human. Another thing make them more prone to attacks because most of the these devices are standalone and if their firmware is not updated at regular intervals it will increase chances of attacks so to avoid this there should be regular firmware updates on all these standalone devices as suggested by manufacturers. Apart from all above suggestion the most reliable approach for IoT security which is suggested by most of the researchers is to divide security into different levels and it will help to stop attackers directly accessing devices most commonly known technique is called the layered approach, Fig. 7 is showing a layered model suggested to avoid direct security attacks on IoT devices.

To elaborate the notion of smart world and its smart components there are many research communities focused on IoT, mobile computing, wireless sensor networks and cyber-physical system. Research in these areas relies on machine learning, real-time computing, security, privacy and signal processing. Fig. 8 is showing authentication procedure through Sequence diagram for QR Based authentication. Our living style and working habits will be changed significantly with the inclusion of these new technological trends. IoT in many different angles cover including architecture, massive scaling, dealing with big data, focusing on security, privacy.

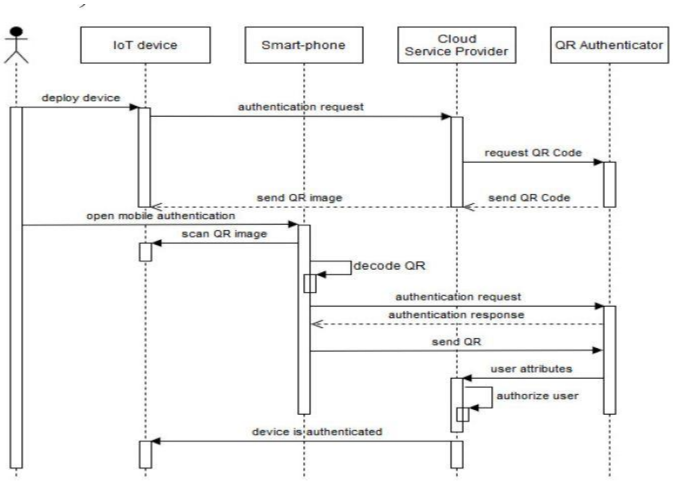


Fig. 8. Sequence Diagram for QR based Authentication.

- **Massive Scaling:** there is a prediction for trillions of devices on the Internet which is going to be a big challenge to deal with security and privacy aspects on such a large scale.
- **Architecture and Dependences:** connectivity such a massive scale devices on internet require a well-defined architecture that allows communication, control, and useable apps.
- **Creating Knowledge and Big Data:** IoT require huge amount of raw data to be collected so there is need to develop technique to convert this data into information. Data mining techniques are used to extract knowledge from sensors data. Another main challenge while extracting knowledge is making decisions while minimizing the false positive and false negative and guarantee safety.
- **Robustness:** In IoT applications sensing, actuations and communication is needed. Each node must be aware of other node's location and synchronized clock. Clock drifts because nodes to have different times resulting in application failure. So for the collections of solutions to create robust systems.
- **Openness:** It means that system is continuously changing and devices have to communicate with each other in this system efficiently. Many sensors and actuators use control and feedback mechanism via controllers.
- **Security:** The fundamental problem in IoT is protection from security attacks. Security attacks create problem due to limited capacity of devices. There must preemptive security measures to protect from these attacks.
- **Privacy:** To solve the privacy problems of IoT the privacy policies of the each system must be specified and enforced accordingly.
- **Humans in the Loop:** Many IoT applications involve humans in the process. Although humans in the loop have many advantages but modeling human behavior is difficult due to physiological, psychological and behavioral aspects

E. *Proposed Layered Security Approach*

Fig. 9 shows proposed block diagram for data collection and its security during transmission of IoT data.

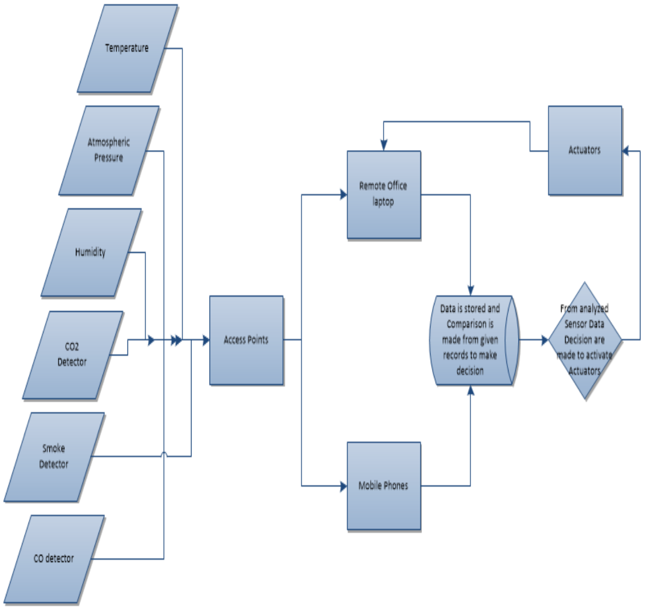

Temperature
Atmospheric Pressure
Humidity
CO2 Detector
Smoke Detector
CO detector
Access Points
Remote Office laptop
Mobile Phones
Data is stored and Comparison is made from given records to make decision
From analyzed Sensor Data Decision are made to activate Actuators
Actuators

Fig. 9. Proposed Sensors Network Model.

Which will be taking sensors for temperature, atmospheric pressure ,humidity, CO2 detector, Smoke detector, CO detectors, these sensors will be transmitting data to any of the near available access points which will be transmitted that data to remote laptop/desktop or on mobile phone. This data will be will further stored in knowledgebase as record for future references and decision making and this analyzed data will be used for decision making to enable actuators which will be further sending updated data to remote computers. Based on nature of communication devices the IoT provides more number of vulnerable points for security breaches to occur, it is very critical to have multi-layers of security. This is because if one of the layers is breached then you must have other mechanisms to fall back on.

V. Discussion and Future Work

This paper discusses different security issues which residents of smart cities are facing and it also provide solution for all these challenges. Future work related to these security issues can be done by registering all the end-user devices in a central data base and all the data stored should be in encrypted form which at one end can increase retrieval time but at the other end it will make sure security of data for all the users who will be using different services provided by smart city administration.

Acknowledgment

I really appreciate cooperation from management of Royal Commission Yanbu and colleagues of University College for facilitating me in setting up lab work.

References

[1] Nasser H. Abosaq, Gasim Alandjani, Shahbaz Pervez. “IoT Services Impact as a Driving Force on Future Technologies by Addressing Missing Dots”. International Journal of Internet of Things and Web Services, 1, 31-37, April-2016.

[2] M. Jahn, Ferry Pramudianto, A.-A. Al-Akkad, “Hydra middleware for developing pervasive systems: A case study in the e-health domain”, January 2009.

[3] Vakali, A., Angelis, L., & Giatsoglou, M. (2013). Sensors talk and humans sense towards a reciprocal collective awareness smart city framework. IEEE International Conference on Communications Workshops (ICC).

[4] Kourtit, K. et al. (2013). 11 An advanced triple helix network framework for smart cities performance. Smart Cities: Governing, Modelling and Analysing the Transition 196.

[5] Pardo, T., Taewoo, N. (2011). Conceptualizing smart city with dimensions of technology, people, and institutions. Proceedings of the 12th Annual International Conference on Digital Government Research (pp. 282–291). ACM, New York.

[6] Giffinger, R., Fertner, C., Kramar, H., Kalasek, R., PichlerMilanoviü, N., & Meijers, E. (2007). Smart Cities: Ranking of European Medium-Sized Cities. Vienna, Austria: Centre of Regional Science (SRF), Vienna University of Technology. Available at http://www.smartcities.eu/download/smart_cities_final_report.pdf.

[7] Giffinger, R., & Gudrun, H. (2010). Smart cities ranking: An effective instrument for the positioning of cities? ACE: Architecture, City and Environment, 4(12), 7-25. Available at http://upcommons.upc.edu/revistes/bitstream/2099/8550/7/ACE_12_SA_10.pdf.

[8] Smart cities: ranking of European medium-sized cities. Centre of Regional Science (SRF), Vienna University of Technology, Vienna, Austria, from http://www.smart-cities.eu/download/smart_cities_final_report.pdf

[9] Shahbaz Pervez, Faheem Babar, Gasim Alandjani, “An Efficient Cloud Model with integrated Services by addressing Major Security Challenges., Journal of World Scientific Engineering Assembly and Society Transactions on Computers Print ISSN: 1109-2750, E-ISSN: 2224-2872.

[10] Leydesdorff, L., & Deakin, M. (2011). The triple-helix model of smart cities: a neo-evolutionary perspective. Journal of Urban Technology, 18(2), 53–63.

[11] Paskaleva, K. A. (2009). Enabling the smart city: the progress of city e-governance in Europe. International Journal of Innovation and Regional Development, 1(4), 405–422.

[12] Al-Hader, M., & Rodzi, A. (2009). The smart city infrastructure development and monitoring. Theoretical & Empirical Researches in Urban Management, 2, 11.

[13] Zygiaris, S. (2013). Smart city reference model: assisting planners to conceptualize the building of smart city innovation ecosystems. Journal of the Knowledge Economy, 4(2), 217–231.

[14] Industry 4.0: the fourth industrial revolution – guide to industry 4.0 http://www.i-scoop.eu/industry-4-0/

[15] Z. Khan, S. Kiani, K. Soomro, "A Framework for Cloud-based Context-Aware Information Services for Citizens in Smart Cities", Journal of Cloud Computing: Advances, Systems and Applications, vol. 3, No. 1, pp. 14, 2014.

[16] M Handte et. Al (2016), “An Internet-of-Things Enabled Connected Navigation System for Urban Bus Riders”, IEEE Internet of Things Journal, Volume 3, Issue 5.

[17] Shahbaz Pervez, Nasser Abosaq, Gasim Alandjani, Adeel Akram, “Internet of Things (IoT) as beginning for Jail-Less Community in Smart Society”, “IEEE International Conference on Electrical, Electronics, Computers, Communication, Mechanical and Computing 28-29 January 2018 at Tamil Nado India.

Author’s Profile

Gasim Alandjani received his PhD Computer Engineering degree from New Mexico State University (USA), He has 27 years’ experience of teaching and research including management experience as Dean, Makkah College of Technology-2003-2009, Deputy Managing Director of Yanbu Industrial College 2010-2012, managing Director of Yanbu Industrial College 2012-2013. Currently, he is working as senior faculty Member in ICT Department at Yanbu University College Royal Commission Yanbu, Kingdom of Saudi Arabia.