Summary

"The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it"

Dr. Mark Weisser, Father of Ubiquitous Computing

How does future world look like? A strive to answer this question has opened up pathways for several outstanding technologies. The Internet of Things (IoT) is the depiction of future internet: comprising of billions of *smart things* interacting and communicating with other machines, objects and infrastructures. IoT is envisaged as one of the most promising upcoming technologies worldwide and is expected that the power to "command and control" things will make human life easier. The IoT also promises to provide countries like India unique handles for e-governance, quality handling of products and food, traffic control, medical assistance to remote areas, tracking origin of drugs, preventing drug counterfeiting etc.

The IoT typically comprises of RFID-Sensing and Embedded Processing nodes connected through wired and wireless communication capability with hierarchical gateways, connected with the cloud. However without proper security mechanisms for all these building blocks, the IoT would not be as pervasive as anticipated. The present project aims to design, evaluate, and deploy the essential security mechanisms for the IoT paradigm. The fact that most of the RFID-nodes, and embedded micro-processors provide platforms which are essentially lightweight and resource constrained imply that traditional approaches of designing complex crypto-solutions will not work. *Physically Unclonable Functions* (PUFs), which are *light-weight, silicon intrinsic solutions* to Hardware Security are an emerging potential solution which can be befitting in the context of IoTs. These designs are often *key-less* and work on the process variations of *nanometer* designs on Silicon. The micro-processor units and the RFID-sensor nodes are furthermore subjected to expert attacks via passive (eg. glitching) and active (eg. UV, electro-magnetics) techniques. The Stuxnet Trojan horse worm that attacked Siemens process control systems at nuclear plants demonstrated high level of malware design and showed the potential damage that can be done to undermine the security of IoT. Combination of active and passive side channels, Trojans, and data analytics in the form of Machine Learning can be catastrophic to the success of IoT. The proposed activity is aimed at designing, analyzing, and deploying suitable strategies to circumvent such threats and make IoT a success. Furthermore, this activity is also aimed at ensuring that our country is ready for future Internet technologies and apply it in a secured manner to solve her several pressing requirements.

1 Thrust Areas and Long Term Goals

Today the Internet is connected to your smartphone. The **Internet of Things (IoT)** will go much further, also connecting your refrigerator, your car, your coffee machine, your door locks, your aquarium, your pacemaker, your lights, your luggage, and your wallet! Although IoT has got tremendous applications for critical infrastructures, as a starting example let us try to envision how the IoT is going to affect our daily life!

Imagine that your alarm clock wakes you up three hours early on a cold winter morning! Your coffee machine is making decaf, while your smart fridge has deep-frozen your milk. Your stereo is playing a melodious number while your lights are strobing "Summer of 69". Your iron has worked all night and has burnt itself out. Your shower seems to work for few seconds and then drenches you with ice-cold water. Your aquarium thermostat has frozen your pet goldfish. A smell is coming from the garden, where your smart heat lamps have set your coveted rose plants on fire! Your robotic vacuum cleaner has grabbed your pet and deposited it in the microwave. Your front door doesn't open while your car is taking a joy ride. Your television set is flashing *Do you want to play a game?* in a spectrum of colors. And to add to it your bank account is empty!!

You are just not having a bad day, You have been *possessed.* Pranksters driving by have sent radio signals that seem to come from your smartphone (violation of authentication), and devices throughout your house have followed the instructions in those radio signals. The Internet of Things has no protection against attack.

Cryptography is designed to scramble communication, making your private messages incomprehensible to eavesdroppers and at the same time protecting those messages against forgery. But fitting cryptography into the Internet of Things poses tremendous challenges. Today's cryptography is too big; today's cryptography is too slow and consumes too much power. This project will explore state-of-the-art efforts to **integrate security into the Internet of Things**, and directions for future research and development.

1.1 General Overview

The Internet of Things (IoT), or the Internet of Objects, refers to the networked interconnection of everyday objects. It is a form of *ubiquitous computing* where the flow of information is envisaged to take place between devices that have traditionally not been required to do so, along with new and novel communicating devices. It is supposed to become an integrated part of our everyday life, to facilitate everyday tasks (both of mundane and critically important nature). In addition, the communication is supposed to be independent of the time, position and nature. In addition to the existing challenges of mobile communication, these requirements create new challenges that must be bed by innovations in protocols, architecture, hardware and software. However, perhaps the biggest obstacle that needs to be overcome is the problem of **ensuring security and privacy** of the information being exchanged. Since most of the information exchange would take place in a seamless manner without user intervention, it is necessary to guarantee that adequate security measures would also be executed seamlessly and without user intervention. But this ease-of-use and seamlessness should not facilitate certain classes of implementation-specific attacks, called **side-channel attacks**, which utilize leaked information to compromise the security of secure systems. It is important to evaluate the effect of side-channel attacks on IoT sub-systems, and to design low-overhead IoT that are sufficiently robust against side-channel attacks. Actual implementation of such seamless and adequate security measures is challenging. There are many factors, but probably the main among them is the computational resource constraints under which the IoT objects, are expected to work. As an illustrative example, *RFID Tags* have been widely proposed and deployed as a simple, unobtrusive and cost-effective system of item identification. However, RFID systems are severely power-constrained. Hence, it is infeasible to execute computationally expensive cryptographic algorithms and security protocols on RFID hardware, which in turn might compromise their security. Similar challenges associated with resource constraints occur for sensor networks, which constitute a very important component of IoTs.

Indian Context: In the context of India and other developing countries, IoTs can revolutionize quality of life. Nano-sensors can be used to monitor water quality at reduced cost, while nano-membranes can

assist in the treatment of waste-water. RFIDs can be used to track the origin of safe drugs thereby reducing counterfeits. Sensor technologies can monitor vulnerable environments and prevent or limit natural disasters. However, given that almost all of the deployed cyber hardware in India is composed of imported sub-components (e.g. imported integrated circuits), it is of paramount importance to ensure their trustability. Use of untrusted hardware components potentially makes the IoT systems vulnerable to hard-to-detect malicious modifications, commonly termed as *Hardware Trojans*. Hardware Trojans can cause disastrous system failures, or leak secret and sensitive information over surreptitious communication channels (information backdoors). In IoTs, this problem is exacerbated by the profusion of communication channels, which would make it difficult to discern malicious communication attempts from benign ones. Hence, it is important to authenticate the hardware sub-systems being used, especially the integrated circuits. **Physically Unclonable Functions** (PUFs) are circuits which have been recently proposed that can act as fingerprint generators for integrated circuits, thus helping to authenticate them. There are several design challenges and reported attacks on PUFs, hence it is important to evaluate their acceptability for IC authentication.

Apart from hardware security related challenges, the IoT network faces a number of security challenges from the IoT communication perspective. Being a low power communication protocol, **IPv6 over Low power Wireless Personal Area Networks** (6LoWPAN) is an attractive technology for IoT communications. However, 6LoWPAN poses a number of security threats and considerations like packet fragmentation attacks, life-logging, bootstraping attacks, frame authentication, secure group communication etc. Such security considerations in IoT communications makes the system vulnerable. The **Datagram Transport Layer Security** (DTLS) is a set of secure Internet communication protocols and architectures for datagram based communications. Despite important security measurements proposed by DTLS, the basic Internet security architecture and the IoT domain still do not fit together easily. This is mainly due to the fact that IoT security solutions are often tailored to the specific scenario requirements without considering interoperability with Internet protocols. On the other hand, the direct use of existing Internet security protocols in the IoT might lead to inefficient or insecure operation.

The growing emergence of Internet of Things (IoT) brings forward a whole array of security challenges. The enormous applications of the IoT to various fields, like healthcare, transportation, Government control, retail and supply chains, energy management, makes it a very promising next generation technology. But amidst the excitement, there are various challenges to be solved: one of the primary hurdles is the issue of privacy and security. Security of Internet of Things is a multi-disciplinary subject, requiring expertises in several disciplines in Computer Science and Engineering. We stress some of the key areas as follows.

1.2 Cryptography and Secured Embedded Architecture

Securing the IoT requires the development of security over the entire path: from sensors to the cloud. The project aims to develop an IoT infrastructure where most of the decisions are done locally, and with minimal access to the cloud. The processing done at the local nodes and at the embedded processors, and the gateways and routers are done at real time with lesser resources (like power, area) available. By security we stress on *information security*: the information that permeates through various parts of the IoT and is context and service dependent. For example, knowing the location of a person would be important, if he or she is lost, while the same should not be compromised when privacy is a concern.

Various applications, like e-Governance, theft controls etc. would emphasize that timeliness of information is maintained. Similarly confidentiality and integrity of data is also to be ensured. Unless data can be trusted it cannot be used for the various applications and the entire system breaks down. The fact that *one is a strong as the weakest link* and the fact that the IoT would encompass billions of devices with various capabilities, architectures and OS, imply that device intrinsic security is imperative. The devices communicate with micro-processor and micro-controller units which can be subjected to various attacks at the physical level: like observe the electro-magnetic signals, perform glitchings, voltage fluctuations (which are feasible in the smart-grid applications of the IoT), perform fault injections via laser beams etc. on the depackaged micro-controllers or FPGAs on which the micro-processors are prototyped. Prior experience shows that conventional ciphers, like AES (Advanced Encryption Standard), ECC (Elliptic Curve Cryptosystems) can be routinely attacked using such side channel sources. Innovative research and development is thus needed

in the area of lightweight cryptography, hardware intrinsic secured VLSI (Very Large Scale Integration) design (like PUFs), and side channel resistance. Prevention and detection of counterfeiting is another key area of impetus for various applications of the IoT.

1.3 Computer Architecture, Computer Networks and VLSI Design

As mentioned before, the overall project involves development of several components. The design of suitable network architectures and micro-processors suited for IoT is an important aspect of the work. To address the billions of devices in the network designs of the IPV6 over low-power wireless area network (6LowPAN) is required to develop the network gateways. While these communication technologies are suitable for several applications like building and industrial applications (at a speed of 250 Kbs) and very low power consumption, there could be applications where other technologies are required, like RFID (400 Kbs), Wi-Fi (11-100 Mbs), 2.5-3.5 G Wireless (1.8-7.2 Mbs). The designs are aimed to be prototyped using Atom boards, FPGAs etc. and subsequently in ASIC technology.

The communication using IPv6 and different web services work as the fundamental building blocks for IoT applications, that support a number of basic advantages like: (i) a homogeneous protocol that allows simple integration with Internet hosts; (ii) simplified development of very different appliances; (iii) an unified interface for applications, removing the need for application-level proxies. Such features significantly simplify the development and deployment of IoT scenarios ranging from smart homes to agricultural managements, where different things such as a sensors and actuators, a luminaire, or an RFID tag might interact with each other, with a human carrying a smart phone, or with back-end services. In the existing literature, security threats have been analyzed in related IP protocols including HTTPS, 6LoWPAN, ANCP, DNS, SIP, IPv6, ND, PANA etc., however the challenge is to analyze their impacts on different scenarios of the IoTs. IoT applications are vulnerable to different attacks over the communication protocols, like eavesdropping, man-in-the-middle, firmware replacement, routing attack and privacy threats, where key exchange materials, security parameters, or configuration settings are exchanged via the open wireless medium. After obtaining the keying material, the attacker may be able to recover the secret keys established between the communicating entities and thereby can compromise the authenticity and confidentiality of the communication channel, as well as the authenticity of commands and other traffic exchanged over this communication channel. Further, An attacker may be able to exploit a firmware upgrade by replacing it with malicious software, thereby influencing the operational behavior of the IoT application. A thrust area of our research is to design secure communication protocols for IoT applications considering resource constraint device capabilities.

Standard micro-processors and micro-controllers also can be attacked using several techniques, like side channels. Power consumption, timing variations due to cache hits and misses, faults through glitching, laser based fault injections can lead to compromise and leakage of useful information. History has taught us that standard architecture designs can be subjected to attacks, and subsequent strategies to add security does not work. As an example, cache based attacks works because of availability of instructions like RDTSC. Now several benign applications have been developed based on this instruction, and hence one cannot stop access to these time stamp counters. There has been recent efforts in top Computer Architecture venues (like ISCA) to fuzz the time stamp counters to prevent these class of attacks. But follow up research from our group shows that they can be still attacked with more sophisticated techniques. These kinds of findings and several others show that the classical Vonn Neumann architecture needs a revisit with security in perspective. Else the weaker links in the IoT will be potential avenues for attacks. Design of processor architectures with security and their VLSI design is also a thrust area.

1.4 Machine Learning

Information exchanged over the IoT generates huge amount of data. The unclonability of PUFs, which are envisaged as the root of trust can be challenged with developments of Machine Learning. These model building attacks can be a potential threat against the promising PUF designs. Literature shows that various PUF designs, ranging from RO-PUF (Ring Oscillator PUFs) to Arbiter PUFs offer various amounts of resistance to such model building attacks. Further the PUF based sensors needs to be registered to the

Micro-processor based readers. The PUFs typically has a huge challenge-response length (more than 64 bits). Maintaining such a huge data-base may be infeasible for the reader. Thus techniques may be researched to enroll by providing fewer challenge-response pairs which can enable the reader to model and obtain the remaining pairs. However the challenge lies in the fact that the adversary should not be able to model based on the challenge response pairs which the PUF based sensor provides. Further developed machine learning based data analysis can be done augmented with side channel sources, like electro-magnetics. The PUFs are also based on publicly available helper data which can be manipulated by the adversary. The subsequent failure rates of the designs can be used to derive the key. All these and several other threats show that the PUF based IoT can be strengthened by suitable machine learning analysis.

2 Long Term Vision

The technologies planned to be developed out of the project is expected to have several far reaching effects. The project aims to develop core expertise in the areas of Security, Embedded Systems, VLSI System Design, Computer Architecture and Networks.

The infrastructure developed can be used for several benefits in the Indian context. The IoT can guarantee ubiquitous, equitable and affordable access to technology, and wider dissemination of service and knowledge. The production and export of commodities can be quality checked by using sensor technologies by tracking their origin, integrity, and tracability. Likewise, the quality and reliability of medical drugs can be ensured through RFID technologies, thus reducing counterfeiting. Diagnosis and treatment of disease, treatment of polluted water and waste water can be affected in a more systematic, controlled and secured manner through a trusted design of Internet of Things. Natural disasters can be monitored triggering early warnings and evacuation. Special sensors and actuators can be developed for the mines thus saving lives and limbs of the workers. Adoption of the IoT will always be influenced by local conditions, and circumstances, thus also influencing the wide spread growth and success of the technology. The present project aims to take the first steps, with security upfront in the design process.

One of the objectives of this work will also be an effort for dissemination of the research and publications in top venues in the area, like IEEE Symposium on Security and Privacy, Cryptographic Hardware and Embedded Systems, Design Automation Conference, Design, Automation and Test in Europe, Eurocrypt, Crypto, Asiacrypt, Indocrypt, Security, Privacy and Applied Cryptography Engineering, Constructive Side-Channel Analysis and Secured Design, , International Symposium on Computer Architecture, Hardware and Architectural Support for Security and Privacy, IEEE Internet of Things (IoT) Journal, IEEE Transactions on Smart Grids, IEEE Transactions on Industrial Informatics, IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Man, Machine and Cybernetics, Embedded Systems Letters, etc.