

ANSPRO TECHNOLOGIES

IEEE 2018-19 PROJECT LIST	
INTERNET OF THINGS(IOT)	
CODE	TITLE AND ABSTRACT
19ANSP-IOT-001	<p>Active Plant Wall for Green Indoor Climate Based on Cloud and Internet of Things</p> <p><i>Abstract</i>— An indoor climate is closely related to human health, well-being, and comfort. Thus, indoor climate monitoring and management are prevalent in many places, from public offices to residential houses. Our previous research has shown that an active plant wall system can effectively reduce the concentrations of particulate matter and volatile organic compounds and stabilize the carbon dioxide concentration in an indoor environment. However, regular plant care is restricted by geography and can be costly in terms of time and money, which poses a significant challenge to the widespread deployment of plant walls. In this paper, we propose a remote monitoring and control system that is specific to the plant walls. The system utilizes the Internet of Things technology and the Azure public cloud platform to automate the management procedure, improve the scalability, enhance user experiences of plant walls, and contribute to a green indoor climate.</p>
19ANSP-IOT-002	<p>Continuous Patient Monitoring With a Patient Centric Agent: A Block Architecture</p> <p><i>Abstract</i>—The Internet of Things (IoT) has facilitated services without human intervention for a wide range of applications, including continuous remote patient monitoring (RPM). However, the complexity of RPM architectures, the size of data sets generated and limited power capacity of</p>

ANSPRO TECHNOLOGIES

	<p>devices make RPM challenging. In this paper, we propose a tier-based End to End architecture for continuous patient monitoring that has a patient centric agent (PCA) as its center piece. The PCA manages a blockchain component to preserve privacy when data streaming from body area sensors needs to be stored securely. The PCA based architecture includes a lightweight communication protocol to enforce security of data through different segments of a continuous, real time patient monitoring architecture. The architecture includes the insertion of data into a personal blockchain to facilitate data sharing amongst healthcare professionals and integration into electronic health records while ensuring privacy is maintained. The blockchain is customized for RPM with modifications that include having the PCA select a Miner to reduce computational effort, enabling the PCA to manage multiple blockchains for the same patient, and the modification of each block with a prefix tree to minimize energy consumption and incorporate secure transaction payments. Simulation results demonstrate that security and privacy can be enhanced in RPM with the PCA based End to End architecture.</p>
19ANSP-IOT-003	<p>A Lightweight Digital Signature Based Security Scheme for Human-Centered Internet of Things</p> <p><i>Abstract</i>—Internet of Things (IoT) comprises of large number of smart devices that can exchange sensed data by availing online services. Smart devices can directly interact with the human beings for sensing the healthcare parameters and transmitting to a central repository. During the data exchange, it is mandatory to secure the messages between sender and receiver to handle the malicious human based attacks. For providing secure communication, a number of signature-based schemes are explored in literature but smart devices need more lightweight operations by ensuring desired security strengths. The main problem during signature based</p>

ANSPRO TECHNOLOGIES

	<p>approaches is the computational overhead due to large real numbers required for signature and verification processes. This paper presents a light weight shortened complex digital signature algorithm for providing secure communication between smart devices in human centered IoT. We have used less extensive operations to achieve signature and verification processes like human beings do signatures on legal documents and verify later as per witness. We have also presented a multi-option parameter selection to use a signature verification pair of expressions at particular index by adopting the common practice of human beings for using different signatures as per document criticality level. It enhances the security strength to guard against traffic analysis attacks. We have developed an experimental setup where a number of cell phones and smart devices are considered for secure communication using existing and proposed digital signature schemes. Results demonstrate the supremacy of our scheme as compared to preliminaries.</p>
19ANSP-IOT-004	<p>RSSI-Based Indoor Localization With the Internet of Things</p> <p><i>Abstract</i> — In the era of smart cities, there are a plethora of applications where the localization of indoor environments is important, from monitoring and tracking in smart buildings to proximity marketing and advertising in shopping malls. The success of these applications is based on the development of a cost efficient and robust real-time system capable of accurately localizing objects. In most outdoor localization systems, global positioning system (GPS) is used due to its ease of implementation and accuracy up to five meters. However, due to the limited space that comes with performing localization of indoor environments and the large number of obstacles found indoors, GPS is not</p>

ANSPRO TECHNOLOGIES

	<p>a suitable option. Hence, accurately and efficiently locating objects is a major challenge in indoor environments. Recent advancements in the Internet of Things (IoT) along with novel wireless technologies can alleviate the problem. Small-size and cost-efficient IoT devices which use wireless protocols can provide an attractive solution. In this paper, we compare four wireless technologies for indoor localization: Wi-Fi (IEEE 802.11n-2009 at the 2.4 GHz band), Bluetooth low energy, Zigbee, and long-range wide-area network. These technologies are compared in terms of localization accuracy and power consumption when IoT devices are used. The received signal strength indicator (RSSI) values from each modality were used and trilateration was performed for localization. The RSSI data set is available online. The experimental results can be used as an indicator in the selection of a wireless technology for an indoor localization system following application requirements.</p>
19ANSP-IOT-005	<p>A Study of Green Development Mode and Total Factor Productivity of the Food Industry Based on the Industrial Internet of Things</p> <p><i>Abstract</i> —Under the background of the rapid development of the global low carbon economy and industrial Internet of Things, building an intelligent and environmentally friendly green industry development mode becomes more and more important. In order to realize real-time, efficient, economical, and environmentally friendly management for resources, and ultimately promote the green production transformation, every enterprise needs to ponder the process of modern industry development. Based on the Industrial Internet of Things, this article discusses the green development mode of the food industry, and uses the entropy method to measure the environmental pollution index of China's food industry. Considering the issue of</p>

ANSPRO TECHNOLOGIES

	<p>environmental pollution and energy consumption, the article uses the DEA-Malmquist method to measure the green total factor productivity of all types of China's food industry from 2006 to 2014. The results show that the environmental pollution index of China's food industry shows a rise — fall — rise trend from 2006 to 2014. The green total factor productivity of Chinese food industry shows a rising trend from 2006 to 2014. The average technical efficiency of China's food industry is low, but the technical efficiency shows a rising trend. The technical efficiency of the agricultural food processing industry remains effective.</p>
19ANSP-IOT-006	<p>A Blockchain Connected Gateway for BLE-Based Devices in the Internet of Things</p> <p><i>Abstract</i>—Recently, the popularity of the Internet of Things (IoT) has led to a rapid development and significant advancement of ubiquitous applications seamlessly integrated within our daily life. Owing to the accompanying growth of the importance of privacy, a great deal of attention has focused on the issues of secure management and robust access control of IoT devices. In this paper, we propose the design of a blockchain connected gateway which adaptively and securely maintains user privacy preferences for IoT devices in the blockchain network. Individual privacy leakage can be prevented because the gateway effectively protects users' sensitive data from being accessed without their consent. A robust digital signature mechanism is proposed for the purposes of authentication and secure management of privacy preferences. Furthermore, we adopt the blockchain network as the underlying architecture of data processing and maintenance to resolve privacy disputes.</p>
19ANSP-IOT-007	<p>IOT Trust-Based Communication for the Industrial Internet of Things</p> <p><i>Abstract</i>—Recently, the Industrial Internet of Things (IIoT)</p>

ANSPRO TECHNOLOGIES

	<p>is attracting growing attention from both academia and industry. Meanwhile, trust-based communication is widely utilized in various systems. In this article, studying the performance of IIoT, we investigate trust-based communication for IIoT. In particular, devoting attention to sensor-cloud, which is a paradigm of IIoT, we propose three types of trust-based communication mechanisms for sensor-cloud. Furthermore, with numerical results, we show that trust-based communication can greatly enhance the performance of sensor-cloud. Eventually, open research issues with respect to trust-based communication for sensor-cloud are discussed.</p>
19ANSP-IOT-008	<p>Privacy Protector: Privacy-Protected Patient Data Collection in IoT-Based Healthcare Systems</p> <p><i>Abstract-</i> In IoT-based healthcare, medical devices are more vulnerable to numerous security threats and attacks than other network devices. Current solutions are able to provide protection to patients' data during data transmission to some extent, but cannot prevent some sophisticated threats and attacks such as collusion attacks and data leakage. In this article, we first investigate the challenges with privacy protected data collection. Then we propose a practical framework called Privacy Protector, patient privacy protected data collection, with the objective of preventing these types of attacks. Privacy Protector includes the ideas of secret sharing and share repairing (in case of data loss or compromise) for patients' data privacy. Since it is the first time, we apply the Slepian-Wolf-coding-based secret sharing (SW-SSS) in Privacy Protector. In the framework, we use a distributed database consisting of multiple cloud servers, which ensures that the privacy of patients' personal data can remain protected as long as one of the servers remains uncompromised. We also present a patient access control scheme in which multiple cloud servers collaborate in shared construction to offer patients' data to healthcare</p>

ANSPRO TECHNOLOGIES

	<p>providers without revealing the content of the data. The privacy performance analysis has shown that the Privacy Protector framework is secure and privacy-protected against various attacks</p>
19ANSP-IOT-009	<p>IoT-Based Sensing and Communications Infrastructure for the Fresh Food Supply Chain</p> <p><i>Abstract-</i></p> <p>Transportation and distribution (T&D) of fresh food is an enormous and growing enterprise due to increasing demand and worldwide sourcing of fresh food. Unfortunately, fresh food T&D not only suffers from significant spoilage and waste but also from dismal efficiency. Here, efficiency is defined as the fraction of T&D capacity that's used. Current T&D efficiency estimates of trucks and trailers are in the 10 to 20 percent range, and food spoilage and waste estimates are in the 12 percent range. Fresh food is easily contaminated, and spoiled or contaminated food is mostly responsible for foodborne illnesses that affect 48 million people annually in the US alone. Supply-chain logistics is transforming because of the current trend of outsourcing operations to a shared third party, or third-party logistics (3PL).¹ Shared logistics is further assisted by several Internet of Things (IoT)-based solutions, such as GS1 standard-based RFID labeling of facilities, locations, products, packages, and carriers. These solutions—along with sensing and communications technologies—enable intelligent T&D. The Physical Internet— an open global logistics system founded on physical, digital, and operational interconnectivity²—encompasses many of these ideas and applies concepts from Internet data transfer to real-world shipping processes. We have extended these concepts to fresh food logistics, ³ demonstrating several similarities to computer networks.</p>
19ANSP-IOT-010	<p>An Innovative Heuristic Algorithm for IoT-Enabled</p>

ANSPRO TECHNOLOGIES

Smart Homes for Developing Countries

Abstract- Over the past few years, active research on algorithm development for the optimal operations of home energy management systems (HEMSs) has been performed. The objective is to compute optimized schedules for shiftable home appliances. This is based on the demand response (DR) synergized with renewable energy sources and energy storage system optimal dispatch (DRSREOD). An improved algorithm for a DRSREOD-based HEMS is proposed in this paper. This heuristic-based algorithm considers DR, photovoltaic availability, the state of charge and charge/discharge rates of the storage battery and the sharing-based parallel operation of more than one power source to supply the required load. The HEMS problem has been solved to minimize the cost of energy (*CE*) and time-based discomfort (*TBD*) with conflicting tradeoffs. The mixed scheduling of appliances (delayed scheduling for some appliances and advanced scheduling for others) is introduced to improve the *CE* and *TBD* performance parameters. An inclining block rate scheme is also incorporated to reduce the peak load. A set of optimized tradeoffs between *CE* and *TBD* has been computed to address multi-objectivity using a multi-objective genetic algorithm (MOGA) with Pareto optimization (PO) to perform the tradeoff analysis and to enable consumers to select the most feasible solution. Due to the rapid increase in demand for electricity, developing countries are facing large-scale load shedding (LS). An innovative algorithm is also proposed for the optimal sizing of a dispatchable generator (DG) that can supply the DRSREOD-based HEMS during LS hours to ensure an uninterrupted supply of power. The proposed MOGA/PO-based algorithm enables consumers to select a DG of the optimal size from among a number of optimal choices based on tradeoffs between the DG size, *CE*, and *TBD*.

ANSPRO TECHNOLOGIES

19ANSP-IOT-011	<p>Open Knowledge Accessing Method in IoT-Based Hospital Information System for Medical Record Enrichment</p> <p><i>Abstract</i>— For a medical treatment with IoT-based facilities, physicians always have to pay much more attentions to the raw medical records of target patients instead of directly making medical advice, conclusions or diagnosis from their experiences. Because the medical records in IoT-based hospital information system (HIS) are dispersedly obtained from distributed devices such as tablet computer, personal digital assistant, automated analyzer, and other medical devices, they are raw, simple, weak-content, and massive. Such medical records cannot be used for further analyzing and decision supporting due to that they are collected in a weak-semantic manner. In this paper, we propose a novel approach to enrich IoT-based medical records by linking them with the knowledge in linked open data. A case study is conducted on a real-world IoT-based HIS system in association with our approach, the experimental results show that medical records in the local HIS system are significantly enriched and useful for healthcare analysis and decision making, and further demonstrate the feasibility and effectiveness of our approach for knowledge accessing.</p>
19ANSP-IOT-012	<p>Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT</p> <p><i>Abstract</i>— The Internet of Things (IoT) is stepping out of its infancy into full maturity and establishing itself as a part of the future Internet. One of the technical challenges of having billions of devices deployed worldwide is the ability to manage them. Although access management technologies exist in IoT, they are based on centralized models which introduce a new variety of technical limitations to manage them globally. In this paper, we propose a new architecture</p>

ANSPRO TECHNOLOGIES

	<p>for arbitrating roles and permissions in IoT. The new architecture is a fully distributed access control system for IoT based on blockchain technology. The architecture is backed by a proof of concept implementation and evaluated in realistic IoT scenarios. The results show that the blockchain technology could be used as access management technology in specific scalable IoT scenarios.</p>
19ANSP-IOT-013	<p>Internet of Things Enhanced User Experience for Smart Water and Energy Management <i>Abstract</i>— Smart environments can engage a wide range of end users with different interests and priorities, from corporate managers looking to improve the performance of their business to school children who want to explore and learn more about the world around them. Creating an effective user experience within a smart environment (from smart buildings to smart cities) is an important factor to success. In this article, we reflect on our experience of developing Internet-of-Things-enabled applications within a smart home, school, office building, university, and airport, where the goal has been to engage a wide range of users (from building managers to business travellers) to increase water and energy awareness, management, and conservation. Driven by the idea of using ICT to more effectively and efficiently manage resources, smart environments have emerged in the form of smart cities, smart buildings, smart grids, smart water, and smart mobility.¹ Mark Weiser and colleagues define a smart environment as “a physical world that is richly and invisibly interwoven with sensors, actuators, displays, and computational elements, embedded seamlessly in the everyday objects of our lives, and connected through a continuous network.”² A key driver in the development of smart environments is the convergence of technologies such as the Internet of Things (IoT) and big data, which are driving the digitization of physical infrastructures with</p>

ANSPRO TECHNOLOGIES

	sensors, networks, and social capabilities. ³ Smart environments, leveraging IoT, can support the development of resource management (for example, water/energy) applications for efficient and effective use of the resource within the environment.
19ANSP-IOT-014	Group-Oriented Range-Bound Key Agreement for Internet of Things Scenarios <i>Abstract</i> — Authenticating the Internet-of-Things (IoT) devices in mobile systems is extremely challenging, because there will be billions of the IoT devices. Most existent proposals only focus on reducing the number of interactions to reduce the authentication overhead. However, there are several critical issues that need to be tackled. In this paper, we address the aggregated authentication overhead issue, the secure key agreement challenges, and the homogeneous trust and authorization issue in the mobile-system based IoT scenarios. Based on the range-bound key assignment technique and our grouping mechanism, we propose the group oriented-range-bound authenticated key agreement to solve these challenges. The main contributions are threefold. First, it drastically reduces the aggregated authentication overhead. Second, it greatly improves the security properties of the key agreement. Third, it facilitates the service providers the fine-grained control of the authentication delegation. To the best of our knowledge, the scheme demands the least authentication overhead among its counterparts; it is the first key agreement scheme that deals specifically with the homogeneous trust and authorization issue and facilitates the dynamic and adaptive authentication delegation. The security properties of the key agreement schemes are verified using a formal security verification tool, the AVISPA, and are analytically proved.
19ANSP-IOT-015	Visualizing the Internet of Things <i>Abstract</i> —

ANSPRO TECHNOLOGIES

	<p>Modern consumer electronics (CE) devices have evolved such that human interaction with machines is ever more natural and effective. The forthcoming deployment of the Internet of Things (IoT) over the existing Internet infrastructure promises to expand this interaction by providing applications and services that allow the human-computer interaction to integrate an automated customization of everyday life [1]. The vision is very optimistic on the amount of smart objects (SOs) deployed around us as the building blocks of the IoT. Experts forecast that 28 billion “things” will be connected to the Internet by 2020 [2]. The IEEE Consumer Electronics Society will likely not be focused on technical details of the IoT (for a detailed technical overview, refer to [3]). It will be of great interest, though, to achieve a level of perception equal to that of natural environments [4]. Armed with their smartphones, the consumers of the IoT will require that SOs be more visible to and interactive with them. Valli [5] argues that system designers should introduce natural interaction models into the next age of interfaces to allow users to switch from the traditional mouse/keyboard pattern to more natural ways of interaction. Since the IoT shifts our attention to physical objects once again, it is important to establish the appropriate interaction paradigms.</p>
19ANSP-IOT-016	<p>iTour: The Future of Smart Tourism <i>Abstract</i>— Smart tourism is an important component of smart cities. However, in many cities, insecurity, safety, fraud, and the lack of availability of proper information about resources are the biggest hurdles toward independent mobility. These issues can be overcome via proactive participation of local citizens to help tourists as well as by cooperation between citizens, city administration, and tourists. As a result, a number of components of smart cities can be strengthened, from sustainable mobility in tourism development to economic</p>

ANSPRO TECHNOLOGIES

	<p>development. This is very challenging, as it requires a combination of societal inputs and advanced smart and effective tools. This article presents a viable Internet of Things (IoT)-based solution called <i>iTour</i> that is a framework for independent tourist mobility. In the process, we analyze the difficulties in initiatives and lessons, exploring possible roles of the IoT.</p>
--	---