

Purdue University
Purdue e-Pubs

Faculty Publications


Department of Computer Information
Technology

1-1-2020

Internet of Things for Sustainability: Perspectives in Privacy, Cybersecurity, and Future Trends

Abdul Salam
Purdue University, salama@purdue.edu

Follow this and additional works at: https://docs.lib.purdue.edu/cit_articles

 Part of the [Consumer Protection Law Commons](#), [Digital Communications and Networking Commons](#), [Health Law and Policy Commons](#), [Internet Law Commons](#), [Privacy Law Commons](#), [Risk Analysis Commons](#), and the [Sustainability Commons](#)

Salam, Abdul, "Internet of Things for Sustainability: Perspectives in Privacy, Cybersecurity, and Future Trends" (2020). *Faculty Publications*. Paper 32.
https://docs.lib.purdue.edu/cit_articles/32

This document has been made available through Purdue e-Pubs, a service of the Purdue University Libraries.
Please contact epubs@purdue.edu for additional information.

Chapter 10

Internet of Things for Sustainability: Perspectives in Privacy, Cybersecurity, and Future Trends



Abstract In the sustainability IoT, the cybersecurity risks to things, sensors, and monitoring systems are distinct from the conventional networking systems in many aspects. The interaction of sustainability IoT with the physical world phenomena (e.g., weather, climate, water, and oceans) is mostly not found in the modern information technology systems. Accordingly, actuation, the ability of these devices to make changes in real world based on sensing and monitoring, requires special consideration in terms of privacy and security. Moreover, the energy efficiency, safety, power, performance requirements of these device distinguish them from conventional computers systems. In this chapter, the cybersecurity approaches towards sustainability IoT are discussed in detail. The sustainability IoT risk categorization, risk mitigation goals, and implementation aspects are analyzed. The openness paradox and data dichotomy between privacy and sharing is analyzed. Accordingly, the IoT technology and security standard developments activities are highlighted. The perspectives on opportunities and challenges in IoT for sustainability are given. Finally, the chapter concludes with a discussion of sustainability IoT cybersecurity case studies.

10.1 Introduction

The cybersecurity in Internet of Things for sustainability is the process of protecting the systems, sensors, and wireless communications from digital attacks [25]. It is important to ensure that the sustainable IoT paradigm will operate in safe and secure environment to achieve sustainability goals using systems which are dependable, reliable, and trustworthy [10, 29, 33]. In many of the sustainability IoT paradigms discussed in this book, the cybersecurity risks to sensors and monitoring systems are different from the conventional networking systems in many aspects:

- The interaction of sustainability IoT with the physical world phenomena (weather, climate, water, and oceans) is generally not found in the modern information technology systems. Accordingly, the actuation (ability of these devices to make changes in real world) based on sensing and monitoring, requires

special consideration in terms of privacy and security. Moreover, the energy efficiency, safety, power, performance requirements of these device distinguish them from computers [89].

- The scale of IoT for sustainable community development expands beyond cities, to the global scale including oceans, climate, and water monitoring applications. Hence, diverse mediums of communications are involved (e.g., satellite, terrestrial air, cellular, and wide area networks) [90].
- Unlike server farms, various sustainability IoT are envisaged to function in harsh and challenged environment for prolonged periods of time without little or no physical access. Accordingly, unconventional security concerns emerge regarding remote access and data privacy [2, 101].
- Lack of upgrade and patching due to high cost is a major challenge as compared to conventional systems [58].
- The sensing data in some of the sustainability paradigms takes longer time to accumulate (such as in climate and agriculture), thereby, presenting prolonged exposure related security challenges [80, 81].
- The implementation of the security features on these sustainability IoT devices requires well-thought design keeping in view its integration in the holistic paradigm and novel insights (security by design) and innovations into the potential risks that can comprise information [33, 43].

In IoT for sustainable community development, it is vital to recognize that sustainability things do not function in a vacuum, rather these are part of the entire ecosystem. Therefore, instead of the individual based security, the holistic approach is of utmost importance. The holistic approach should take end-to-end strategy for cybersecurity across the entire sustainability landscape [33, 54]. Moreover, within each sustainability paradigm, each system has its own specific function and purpose with its ability to tolerate risks. Hence, no single cybersecurity protocol or set of rules can be applied to entire paradigm. These risk mitigation approaches vary based on system needs, functions, and use cases.

Accordingly, it is import to underscore the characterization of risk-based insights into functionality, deployment environment, set of behavior and applicabilities and their integration into the paradigm [7]. In this regard, the outcome based cybersecurity approach can be applied where the final outcome becomes more important as compared to less significant means to achieve those outcomes. The examples of weaknesses and unreasonable cybersecurity approaches towards sustainability IoT are discussed in the following [44, 53].

- Data and information storage in plain text
- Negligence in adequate policy implementation
- Oversight of in fixing current vulnerabilities
- Failure to utilize proper cybersecurity protocols
- Neglect of modern technology for protection such as firewalls
- Omission of network access regulations
- Lack of adequate incident response protocols

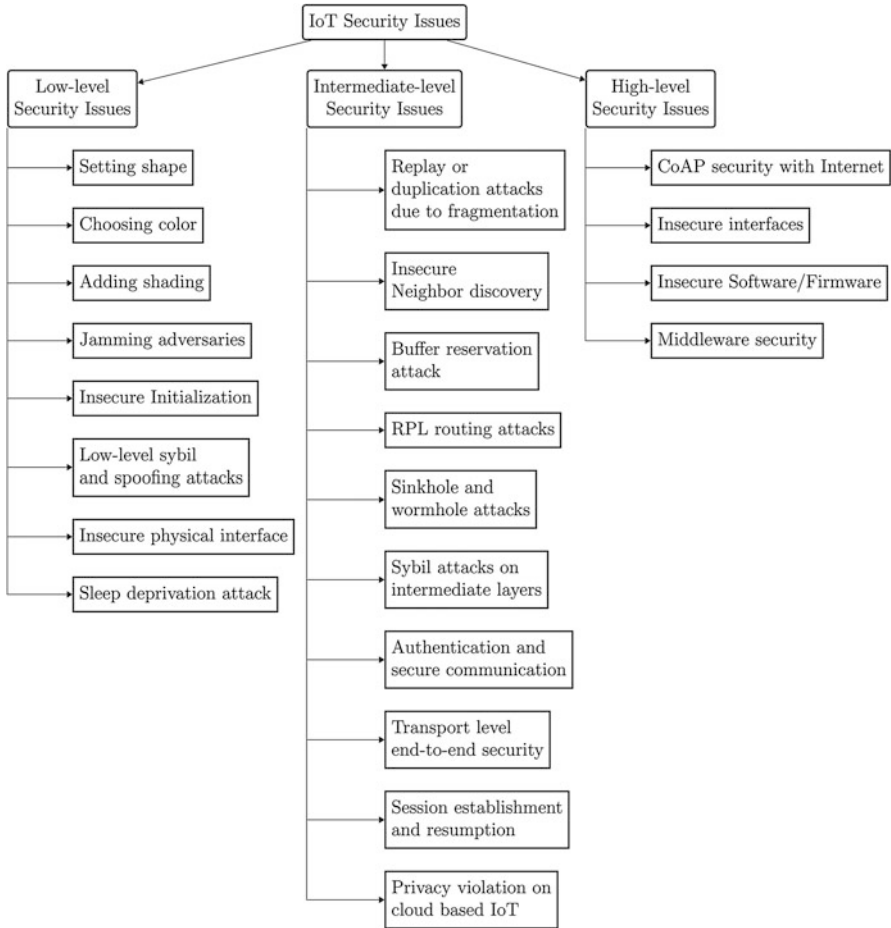


Fig. 10.1 Security issues in IoT [44]

In sustainability IoT, both the device and data security are of vital importance. Different security issues in IoT are shown in Fig. 10.1.

Device security deals with protecting IoT devices from attacks, whereas the data security is related to protection of data integrity and confidentiality being generated from IoT sensors and other monitoring instrument. This also applies to the user privacy. The first step towards the securing IoT devices is risk identification and categorization, in which the impact of different IoT devices is considered. A three-pronged stratagem can be employed to identify risks, which include utilitarian, feasible, and verifiable. The first prong follows the utilitarian principle to identify the practical importance and appropriateness of risk. Then feasibility principle analyses the implementation complexity, cost, and verifiable details which deals with the implementation verifiability. In this process, both

sustainability IoT functionality and cybersecurity needs are considered (device usage and management, configurations, networking capabilities, nature of data collection storage, access and actuation capacity). These risk identification and categorization includes [29]:

- A major factor for sustainability IoT risk categorization is consideration of things based on their information related capabilities [29]. The sustainability IoT can be characterized into active and passive. The examples of the passive devices, which have no actuation capability, include water pH and nutrients sensors, in sustainable water IoT, soil moisture sensor in sustainable agriculture IoT. The active things collect data and also act as actuator to make changes in the physical world. The examples of active things include center pivot systems controllers based on soil moisture sensing which are used in sensor-guided irrigation management systems and also in reservoir monitoring for flow control in dams.
- The physical accessibility of sustainability IoT is considered to establish the risk category. For example, underground soil sensors for monitoring physical, chemical, and biological properties of soil in decision agriculture are hard to locate, access, and excavate. Similarly, sensors in ocean floors, rivers, and other water bodies, in urban underground infrastructure, and mines are difficult to access. The remote access and authentication features should also be identified.
- The communication capabilities of these devices from short range to very long-range communications using different mediums such as central offices wire line, wireless, cellular networks, cable and broadcasting systems, and satellite communications should also be considered for risk categorization. Each of these communication mediums present diverse challenges in terms of risk identification. Moreover, the types and duration of data collection transmission should be analyzed to characterize risks.
- The power source and energy efficiency are vital for sustainability IoT risk characterization. The things can be either battery powered or hard wired. Accordingly, energy harvesting mechanism and power transfer mechanism to enhance battery life should also be considered [37].
- The IoT authentication capabilities, device software graduation, and patching approaches are also used to determine risks. It includes system and network authentication and device access identification. The personally identifiable information (PII) poses high risks [95].
- The sustainability IoT firmware and software modules complexity and configuration are also fundamental components of the risk identification and categorization [18].

Accordingly, based on sustainability IoT risk categorization, the risk mitigation goals and areas are defined based on the significance of the risks categorization identified in the first step. These risk mitigation challenges, recommendations in different areas are discussed in the following [16, 67]:

- To prevent unauthorized access to system, adequate logical and physical access procedures should be instituted using the state-of-the-art authentication mechanisms. Moreover, all access and use of resources by anyone should be logged properly for proactive avoidance.
- For the purpose of efficient management of cybersecurity risks, a database should be maintained for IoT and their operational characteristics (firmware version, services, functionalities, and software version) as discussed above. This should also include all relevant information about the device status.
- Keeping track of software and hardware vulnerabilities is useful to reduce exposure of system to digital attacks. Accordingly, these vulnerabilities can be fixed by employing a systematic approach.
- The data generated from all phases of sustainability IoT life cycle should be protected at all stages during sensing, collection, transmission, analysis, and visualization from manipulation and compromise by using best cryptography and security practices.
- A continuous monitoring of data and devices is important to identify any incidents of data and security breaches, vulnerabilities, and bugs.

The next step in securing sustainability IoT paradigm after identification of cybersecurity goals and areas is implementation of these goals (also called the cybersecurity feature implementation). This process is performed considering the technical specifications of sustainability things (e.g., hardware needed to support a particular feature keeping in view the current in future needs). The emphasis is on hardware based feature implementation because of efficiency and use of some of the existing built-in features in the devices. A cybersecurity risk management roadmap is shown in Fig. 10.2. In this process, system performance is also monitored to identify any adverse impacts of the features. The adoption of a system level approach has tremendous potential where all elements of the sustainability IoT are considered such wireless communications and interaction with other things. For example, precision agriculture cybersecurity features should be implemented considering all farm equipment and privacy issues [1].

There are many common security vulnerabilities that go unnoticed during development and shipment phase. The update related issues that are generally observed include user/devices never getting an update (inability in terms of device capabilities), failure of the vendor to send updates (due to absence of autonomous sending patches and updates), and users failure to apply updates.

Moreover in the absence of adequate authentication and encryption mechanisms in place, the update and patch push approach is unlikely to be successful because of security issues and devices can be compromised. Moreover, data theft issue can happen at unsecured device (no or plain text passwords), cloud (man in the middle attack), and network communications levels (no encryption) The detailed IoT security considerations at different levels are outlines in the following:

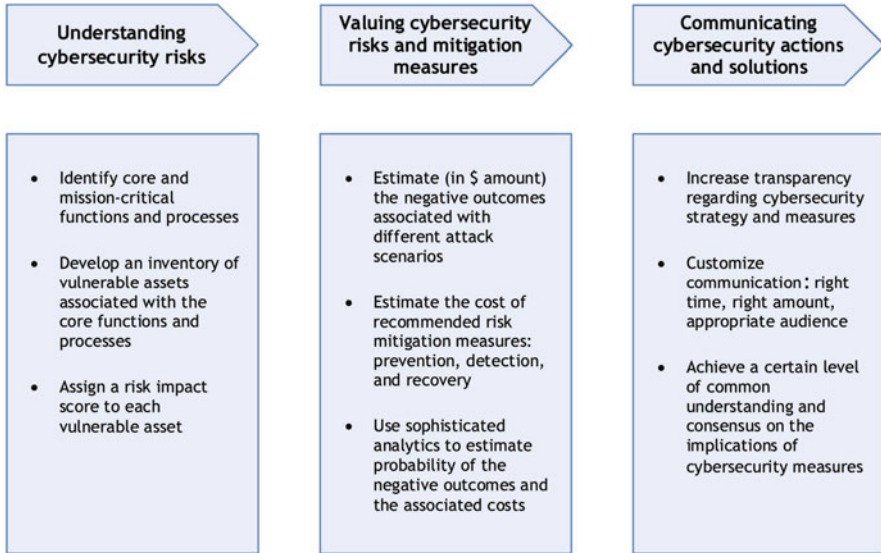


Fig. 10.2 A cybersecurity risk management road map

- At data and application layers in IoT Applications: It includes malware, theft of data, unauthorized access, man-in-the-middle attacks, unauthorized software, spoofing, fraud, denial of service, and inconsistent software versions.
- At networking level: It includes denial of service, spoofing, protocol tampering, hijacking, clear text communications, false base station, man-in-the-middle attacks, and lack of monitoring.
- At device level: It includes back doors and call home functions, reverse engineering, unauthorized software, side channel, device cloning, proxy acts, and resource limitation.

10.1.1 *IoT Security Principles*

The U.S. Department of Homeland Security in its report Strategic Principles For Securing The Internet Of Things (IoT) has defined following principles to address IoT security challenges [25]:

- Incorporate Security at the Design Phase
- Advance Security Updates and Vulnerability Management
- Build on Proven Security Practices
- Prioritize Security Measures According to Potential Impact
- Promote Transparency across IoT
- Connect Carefully and Deliberately

10.1.2 Digital Forensics in Sustainability IoT

The digital forensics in sustainability IoT deals with the investigation of data on IoT and digital devices related to legal matters and computer crime. Currently, there is no standard set of guidance for data retrieval for the purpose of the litigation investigation in case of cyber comprise, theft, or other crimes. To meet this requirement, there is a need for collaboration to cyber, digital, computer, and network forensics experts, industry, and government authorities.

10.2 Openness Paradox and Data Dichotomy: Privacy and Sharing

In sustainability IoT, data collected at large spatial, temporal, and environmental scales carries a huge economic value. The openness and data flow are of vital importance for decision support systems and for developing sound data driven practices, and at the same time requires protection as well [31]. In this section, the challenges of data sharing and privacy in sustainable IoT are discussed in detail.

10.2.1 Privacy in Sustainability IoT

The identification of privacy regime and concerns is important in sustainability IoT due to the sensitive nature data in sustainability IoT. Due to its large-scale sensing and data monitoring capabilities, the enormousness amount of data is being generated in different paradigms such as climate, water, energy, and health. In this regard, the data privacy and protection is being considered pivotal for successful functionality of the system. However, different IoT generate different amount of data. One big motivation for protecting data is to avert users data being revealed and to block circulation of protected information. For the first case, well-designed sifting approaches can be used to curb revealing individual information. For proprietary information, formation of proper training is vital to protect dissemination of the data.

10.2.1.1 Data Sifting

Data sifting is an important privacy mechanism to ensure privacy and achieves balance between the scenarios of no data sharing at all and everything being shared. This approach also ensures that the important information and data about climate change, water, and health related issues while protecting the privacy of individuals

(e.g., age, name, address, location, and social security numbers). However, by removing this information entirely makes gender, age, and location based analysis impossible to conduct.

Another important privacy achieving mechanism also called the differential privacy includes adding a well calculated noise to the aggregated understudy data set such that results are twisted to make identification of the individuals difficult. In this approach, the exact data is replaced with range and data granularity is reduced statistics based data summarization. The quantity and quality of noise depends on the size of data set being analyzed. Accordingly, machine learning [15] can be used for data mining and to construct models from the data. An aggregation approach is shown in Fig. 10.3.

10.2.1.2 Proxy Data Analyzer

In this approach, intelligent proxy data analyzers are used to process data based on the data request. This approach enables selective data sharing across different domains based on metadata, data sensitivity, and previous requests. Using proxy data analyzer, multiple sustainability IoT data sets can be combined to regional to universal planning. The FLEX is an example of proxy data analyzer that provides differential results by using a set of precomputed data metric. These privacy-preserving approaches will enhance end user trust in system, hence removing barriers in technology adaption by encouraging innovation.

10.2.1.3 Multi-Layered Approach to Privacy

In a multi-layer approach to protect privacy in sustainability IoT paradigm, each layer can guard against the specific set of data being revealed. For example, data element encryption added an additional layer of protection. Similarly, at the session and presentation layers, use of encryption mechanisms is useful to mitigate attacks conducted during data communications. In summary, the strong privacy protections will be helpful to advance the sustainability IoT paradigm.

10.2.2 Universal Data Flow, Sharing, and Standardization

The open flow of data and sharing coupled with best management practices brings tremendous value to sustainability IoT and is the lifeline of the entire ecosystem. The design of new data sharing platforms for sustainability has the potential to bring robust policy planning and decision making in different areas such as environment.

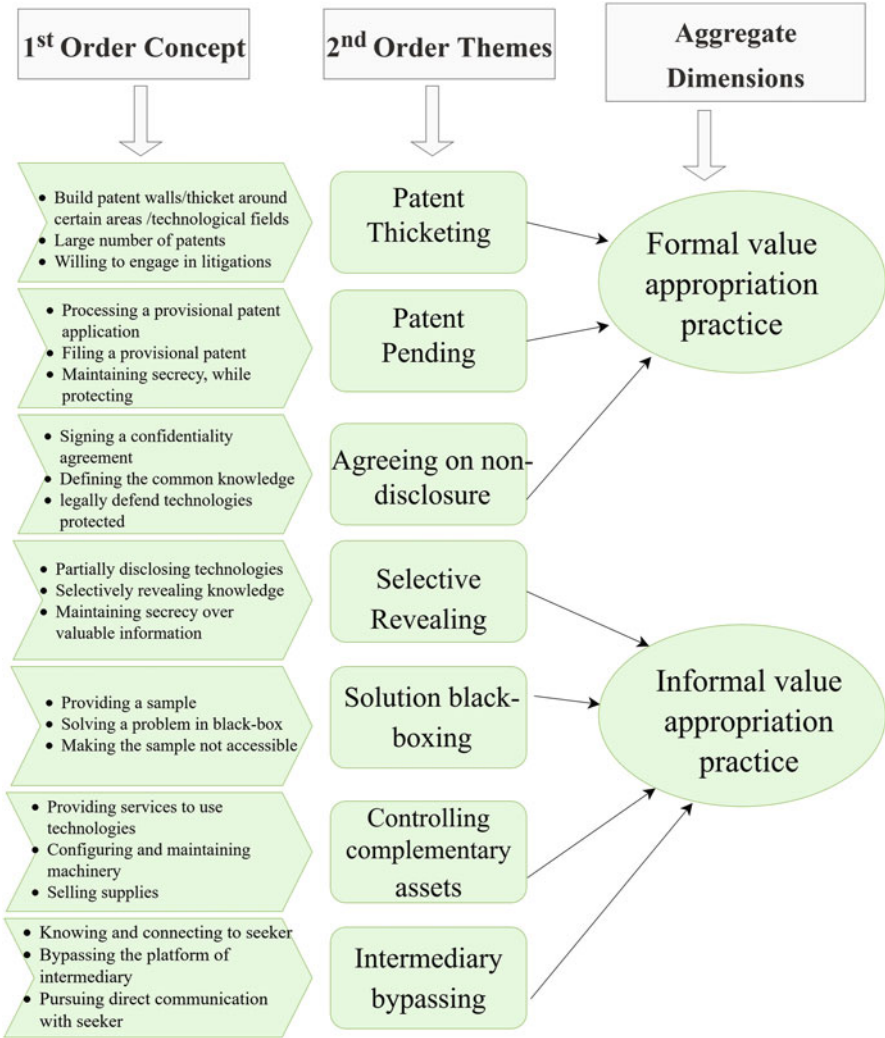


Fig. 10.3 An analytical aggregation approach [31]

10.2.2.1 Significance of Data Sharing

The data localization inhibits global scale mitigation, cross-border forecasting, and planning efforts, whereas more socioeconomic and environmental benefits can be realized by global sharing. For example, in energy sector, loads can be identified and proper system planning can be done. Similarly, in health sector, the underlying causes of spread of a particular disease in affected communities can be established, which will also be beneficial for world population at large to prevent disease outbreak. In transportation, better public services can be designed. Similarly, the

availability of timely and certain data has a vital role to play in improving the urban underground infrastructure monitoring. It can also facilitate the development of monitoring systems for sewer and storm water overflows through real-time operation. The data localization also presents a barrier to international adoption of different sustainability IoT paradigms. In this regard an establishment of a global cloud for sustainable IoT will be good step in the right direction. The data flow and sharing can be conducted at two levels.

- At strategic level (community and large geographical level): to give certain pertinent data about the community to policy makers for analysis and strategic decision making
- At tactical level: for local operation, planning and forecasting and behavior identification to understand and address the societal, social, and environmental issues and challenges.

10.2.2.2 Data Standardization

The deployment of sustainability IoT devices in different infrastructures with multitude of sensors and instruments provide many tremendous avenues for valuable data collection. The data collection from different sustainability IoT can be classified into (1) exhaust, (2) sensing, (3) crowdsourcing, and (4) web-based. However, different schematics and data access procedures, variations in data storage formats, difference in spatial and temporal granularity present big challenges in combining, comparison, analysis, and interpretations of these data sets.

The data standardization deals with data storage and management using reliable mechanisms in structured format to enable large-scale data analytics. The availability of structured data makes it extremely easy to make futuristic predictions. Accordingly, advanced data analytics can be used to predict, estimate, diagnose, and prognose events and outcomes from past and current data flows in real time. It also enables a consistent aggregation of data across different sources and places. Accordingly data-driven and analytical models can be developed in different areas related to sustainability (e.g., renewable energy profiles, weather forecasting, water monitoring planning, and analysis for sustainable community development).

10.3 Opportunities and Challenges in IoT for Sustainability

The IoT has strong potential to transform different sustainability areas using sensing and communications technology. It is capable of effectively responding to the current environmental, energy, water, and health challenges using the technology and hence can achieve the sustainability goals and bring improvements to quality of life. Its sensing and monitoring brings benefits to the society by fixing environmental issues, and also guides regulations and policy making. For example, sensors in

water bodies are used to obtain useful information about the quality and flow of water, which helps in waste and treatment management. Similarly, soil sensors provide useful information about the physical, chemical, and biological properties of the soil which aids in improving crop yield and water resource conservation. Yet, bountifulness of these opportunists comes with many challenges at the technical level and policy level. These challenges are discussed in the following section.

10.3.1 Technical Challenges

The challenges in IoT for sustainability are:

- Sustainability Data management. Novel approaches are needed for data collection, storage, sharing, and analysis due to size, scale, and distributed nature
- In privacy and cybersecurity, and equitable access regarding exposure, manipulation, and misuse of critical data
- Lack of encryption, resources for a certain level of protection, privacy guidelines, and protection against malicious cyberattacks
- Sustainability device homogeneity increases vulnerability of cascading and repetitive attacks
- Existing public infrastructure compatibility and integration issues. Lack of interoperability (at network, system, and data formatting levels) causes data silos, redundancy, and inefficiency

10.3.2 Policy Challenges

Smart global and national strategy for public regulations and policies, based on environmental, social, and economic factors are critical for the success of sustainability IoT to deal with huge challenges in meeting sustainable development goals. The policies developed using collaboration and civic engagement will have strong impact on sustainability. The policy level challenges and sustainable actions recommendations are discussed in the following section.

- Need of inclusive collaboration and civic engagement planning among different sectors keeping in view the current and future needs. For example, sensing in one area has the potential to meet the needs of other area too (e.g., carbon dioxide emissions in energy, climate, and transportation). In this regard engagement with public, academia, and private industry is also of vital importance to develop and deploy the state-of-the-art technologies.
- Community engagement should also be focused on people participation and citizen engagement. The sustainability things will be useless and wastage of resources and other infrastructure if citizens are unable to use the system. In this regard, providing access and expansion of services to rural broadband

will certainly increase access to these systems. The constituency resources and demographics are of fundamental importance for the planning and deployment purpose.

- Policies for data access, ownership, and stewardship.
- Policies to mitigate behavior change resulting from the deployments of sustainably IoT systems.
- Development of trust and reliability frameworks.

10.4 Progress in IoT Security Standardization

The full potential of sustainability IoT will be realized only if it operates in an open and secure environment. Different security groups and industry are developing technology and security standards to promote interoperability, and to encourage open and secure cross-border data communications. The different technology and security groups for IoT and their standardization efforts are discussed in Table 10.1 [98].

10.5 Case Studies

In this section, different sustainability IoT cybersecurity case studies are discussed. First, the case study of cybersecurity and data privacy in digital agriculture is presented.

10.5.1 *Cybersecurity and Data Privacy in Digital Agriculture*

The digital agriculture has been envisaged as a novel archetype to transform present-day agricultural practices by real-time sensing, processing, and collection of data for the purpose of developing efficient seeding and irrigation techniques, fertilizer applications, and other farm operations [3, 9, 27, 36, 52, 70–78, 80, 82–87, 93, 96]. Many security threats are emerging in the nascent field of digital agriculture (also referred to as decision agriculture and precision). In digital agriculture, various types of sensing and communication technologies are used (e.g., in situ sensing, remote sensing, machine learning, and data analytics.) Hitherto, the agriculture field was dependent on mechanical device and technology use was minimal. Accordingly, by using these networked technologies for sensing and data collection, different types of field inputs such as water for irrigation, fertilizer, and pesticides can be applied precisely in agricultural farms that improve efficiency, bring enhancements in crop yield, and lower costs. However, with this rapid growth of agricultural technologies, there is corresponding increase in vulnerabilities. In this section, we discuss those vulnerabilities, prospective threats, and solutions.

Table 10.1 The IoT technology and security standard developments activities [98]

Organization	Description
IoT Cybersecurity Alliance	A group of industry leading cybersecurity and IoT experts to help address the challenges that exist across the IoT ecosystem
Cloud Security Alliance	Best practices and research
Alliance for Internet of Things Innovation	It aims to strengthen the dialogue and interaction among Internet of Things (IoT) players in Europe, and to contribute to the creation of a dynamic European IoT ecosystem to speed up the take up of IoT.
Broadband Forum	A non-profit industry consortium dedicated to developing broadband network
European Telecommunications Standards Institute (ETSI)	Produce applicable standards for ICT-enabled systems, applications and services deployed across all sectors of industry and society
GSMA IoT Security Guidelines	It include 85 detailed recommendations for the secure design, development, and deployment of IoT services that cover networks as well as service and endpoint ecosystems. It addresses security challenges, attack models, and risk assessments while providing several worked examples.
IEEE Internet of Things	Security and Encryption Standards. IoT security issues and vulnerability.
Industrial Automation and Control System Security	It develops security standards and technical reports.
Industrial Internet Consortium (IIC)	Security-related architectures, designs and technologies.
International Electrotechnical Commission (IEC)	International Standards and Conformity Assessment for all electrical, electronic, and related technologies
International Organization for Standardization (ISO) IoT Standards	Develops standards for security
Internet of Things Consortium	IoTC is a non-profit member based organization connecting a global ecosystem of leading companies building the Internet of Things
IoT Security Foundation	IoTSF is a collaborative, non-profit, international response to the complex challenges posed by security in the expansive hyperconnected world
ITU-T SG20	An emerging standard
National Institute of Standards and Technology	CPS PWG cyber-physical systems (CPS) framework, and NIST cybersecurity for IoT program
North American Electric Reliability Corp	Responsible for reliability and security of the bulk power system in North America
oneM2M	It is a global standards for machine to machine communications and the Internet of Things.
Online Trust Alliance	OTA is convener of a multi-stakeholder initiative to address public policy and technology issues impacting IoT devices.

(continued)

Table 10.1 (continued)

Organization	Description
Open Connectivity Foundation	The open connectivity foundation (OCF) is a group of over 300 technology companies, including Cisco, Intel, and Samsung, and is developing interoperability standards for the IoT and sponsoring an open source project to make this possible.
Open Mobile Alliance (OMA)	OMA device management security describes general security requirements, and provides description of transport layer security, application layer security
Open Web Application Security Project	The OWASP Internet of Things project is designed to help manufacturers, developers, and consumers better understand the security issues associated with the Internet of Things, and to enable users in any context to make better security decisions when building, deploying, or assessing IoT technologies.
OpenFog Consortium	Enabling advanced IoT, 5G and AI with fog computing
SAFECode	The software assurance forum for excellence in code (SAFECode) is a non-profit organization dedicated to increasing trust in information and communications technology products and services through the advancement of effective software assurance methods.
Smart grid interoperability panel (SGIP)	SGIP is an industry consortium representing a cross-section of the energy ecosystem focusing on accelerating grid modernization and the energy internet of things through policy, education, and promotion of interoperability and standards to empower customers and enable a sustainable energy future.
Thread Group	Thread was designed with one goal in mind: to create the very best way to connect and control products in the home
The Update Framework (TUF)	The update framework (TUF) helps developers to secure new or existing software update systems, which are often found to be vulnerable to many known attacks.
U.S. Food and Drug Administration (FDA)	Management of postmarket cybersecurity vulnerabilities for marketed and distributed medical devices
US Department of Homeland Security (DHS)	Strategic principles for securing the Internet of Things
3rd Generation Partnership Project (3GPP)	A global initiative that unites seven telecommunications standards development organizations (known as “organizational partners”), the 3GPP develops specifications covering cellular network technologies, including radio access standards.
Internet Engineering Task Force	IoT Standards
CIS Center for Internet Security	CIS is a forward-thinking nonprofit that harnesses the power of a global IT community to safeguard public and private organizations against cyber threats.

It is important to note some of the common threats (e.g., malware, theft of data, unauthorized access, man-in-the-middle attacks, unauthorized software, spoofing, fraud, denial of service, and inconsistent software versions) found in conventional connected systems also pose risks in the field of digital agriculture [28, 69]. Therefore, these can be identified by using the conventional risk characterization approaches discussed in this chapter, and, accordingly the same established risk mitigation can be applied. However, due to distinctive operation of the farm machinery, equipment and underground sensors, vast area of exposure from field to farms, various type of new threats are emerging which were not observed previously with wide range of ramifications. These consequences range from interference to routine field work to total disruption and unavailability of farm operations and compromised integrity and confidentiality of farm data. Moreover, the data leakage and theft negativity impacts the agricultural resiliency and sustainability.

10.5.1.1 Information Privacy in the Field

In digital agriculture, the data privacy is a major issue in relation to technology implementation. Recently, plenty of critical data has been collected by farmers about their farms such as crop yield data which they are reluctant to share due to different factors (e.g., finance, market trends, and soil value) [104, 105]. Across a typical agricultural farm, many variations in soil texture, nutrients, and volumetric water content are observed [76]. The agricultural technology is used in these temporal and spatial variations to ascertain field conditions for variable applications of fertilizer and irrigation in order to maximize yields and profits which provides financial gains to farmers. To determine field conditions for best resource allocation, various technologies (e.g., GPS, GIS, and sensors are being used) where data can be collected and stored in cloud for processing.

Since, at large spatial scales, the soil texture and rain data is highly correlated, the cloud data collected from multiple farms can be utilized for decision support systems at regional levels. For example, soil moisture data along with temperature across different farms can be used to inform irrigation decisions [27]. Consequently, with this benefit, the data privacy becomes a concern particularly in geo-spatial usage of privacy information [20]. For the reason that location data is used by vendors, dealers, and digital agriculture service and equipment providers for developing analytics, improving service and for creation of new business models; the security threats and attacks make the farmers data exposed and vulnerable.

Such security breaches are detrimental as not only the farm's equipment and sensing data is revealed, the other proprietary information is laid bare such as irrigation cycles conducted in a typical growing seasons, software design and version, seeding approaches, and yields. Since, the success of the farming depends on these, therefore, the farmers keep these information confidential. Currently, in the developing area there is dearth of mechanisms to protect data privacy [49]. One privacy protection mechanism that has applications in this area is obfuscation

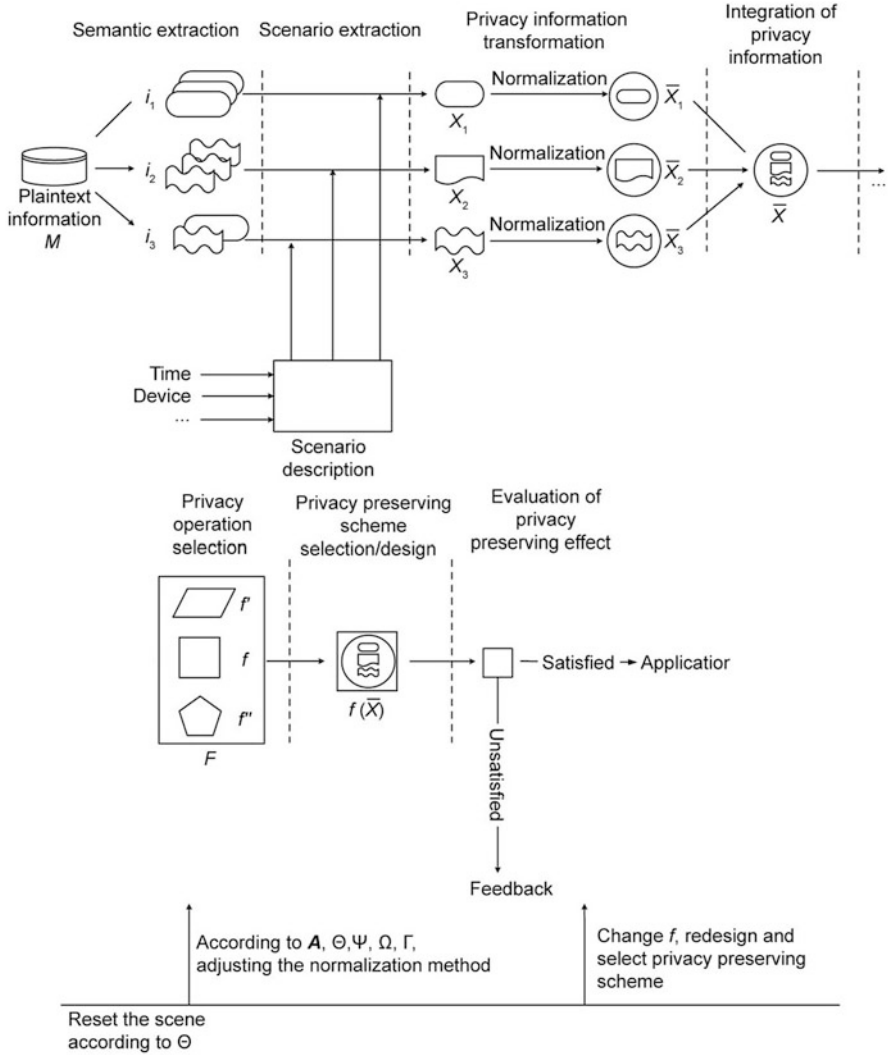


Fig. 10.4 A privacy computing framework [49]

(see Fig. 10.4) where exact location information is replaced with confusing and ambiguous information. However, this will render geographic services unable to function because of lack of true data. Moreover, the obfuscation techniques are also vulnerable to the location deduction attacks. Thus, in digital agriculture, advanced mechanisms to protect privacy and location information without surrendering the location information are needed.

Farm data privacy related threats in digital agriculture are discussed in the following [30, 105]:

- Deliberate stealing or unintended leakage of farmers information from decision making systems and other agricultural information management systems to third parties. This targets mobile and tablet apps on the farm equipment and farmers phones. Currently, these applications lack update features and privacy protection mechanisms [91, 105].
- The purposeful publicizing of information to harm a company's reputation and sow mistrust about technology in farmers' minds leads to hindrances in adaption of decision agriculture [105].
- The exploitative trading of confidential data, where companies are approached to sell farmers data in return for some incentives [34].

10.5.1.2 Data Usability in the Field

In digital agriculture, sensors are being used for condition monitoring and real-time decision making at different temporal and spatial scales that cause data consistency issues. These challenges are discussed in the following [75]:

- Publishing of false data about crop disease or other related agriculture to create fears among farmers [69, 105].
- Injection of false data into the sensing networks to create false alarms or trigger harmful actuation such as over irrigation and under irrigation [80, 88].
- Inefficient control algorithms for farm machinery and other in-field equipment.

10.5.1.3 Farm Equipment and Data Availability in the Field

Because agricultural farm operations are heavily dependent on the farm equipment therefore, the data loss is the major challenge in the field. In this major disruptions to the availability are:

- There are some critical time windows in every crop where the of equipment usage is at its peak such as combines in the harvesting systems, center pivot, seeders during planting season, and drip irrigation systems in long dry weather or short-term droughts. Loss or malfunction of equipment during these intervals is detrimental to the crop health. It can also cause crop yield reduction leading to the financial loss to farmers. Attacks conducted to exploit vulnerabilities in the equipment can cause large-scale food shortage and harm the vendors reputation [6].
- The overcrowding of wireless spectrum can cause disruptions to the wireless systems and GPS signals in the agricultural farms. The overcrowding of the spectrum can also lead to improper and unpredictable functionality of the system.

The Federal Communication Chart (FCC) has permitted the use of the cognitive radio devices in the spectrum range of 470 to 698 MHz on farm machinery and agricultural equipment for digital agriculture applications [79].

- The limited availability of rural broadband leads to loss of data, slow data rate, maintenance downtime, and frequent service outages. The wireless communications can also be used to exploit the data being transferred in plain text [61].

10.5.1.4 Cybersecurity Recommendations for Precision Agriculture

Some important recommendations for protection of precision agriculture systems in the field are discussed in the following [17, 51, 103]:

- Security of applications and software being used in the field on farm equipment can be achieved using latest updates, patches, and security mechanisms [92]
- Blocking of communication loopholes by using strong encryption standards for data transfer, and blocking services and protocols not required for device functionality. The implementation of the latest security standards will also reduce risks [12]
- An updated record of device functionality, software, and current status. The continuous monitoring and logging of the device access to verify authorized users. Understanding of data ownership, protection, and recovery protocols is also useful to develop proper incident response strategy

10.5.2 *Smart Grid*

In modern smart grid systems disruptions in one system can lead to cascading effects in the entire power system [40]. The cyberattacks in grid can cause substantial losses. There is strong need to increase the reliability of these systems by protecting them from cyberattack by incorporating the cybersecurity in the design process. This can be achieved through development of reference security architecture. An example of cybersecurity architecture for the power grid is shown in Fig. 10.5. The design of the next generation power grid system including renewable energy systems can benefit from this which is based on the IP networking.

10.5.3 *Health and Cybersecurity*

The cybersecurity vulnerabilities and threats can affect the availability of critical lifesaving medical equipment and data. The cybersecurity threats can cause physical impact in patients, hinder the regular hospital operation leaving them unable to provide care [14, 35]. Therefore, attaining the highest level of cybersecurity in

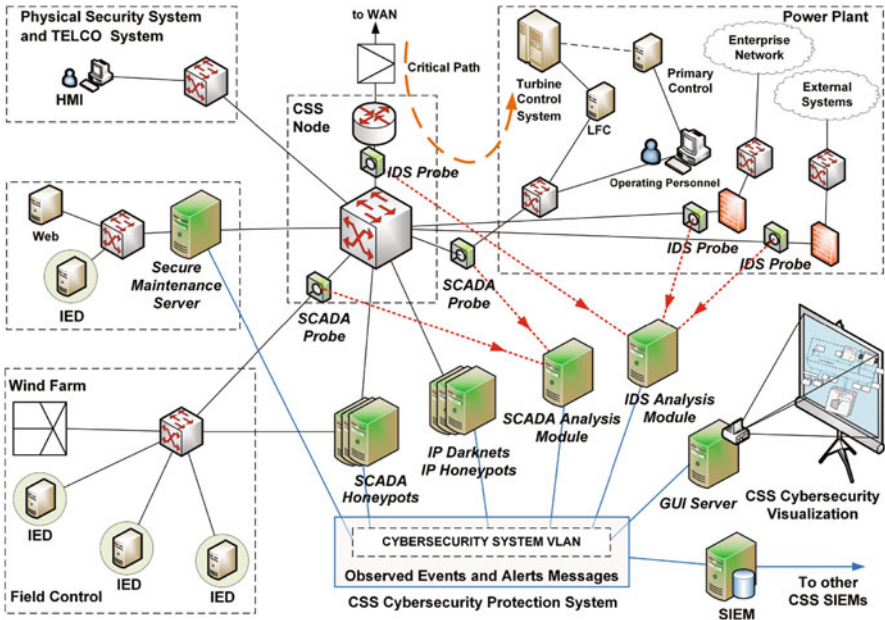


Fig. 10.5 A power grid control system and the designed cybersecurity protection system [40]

healthcare is important for patient safety. The identity theft, ransomware, and targeted patient hacking are some of the vulnerabilities. Other issues are addressed in the following section.

10.5.3.1 Critical Conditions of the Healthcare Cybersecurity

The challenges being faced by the healthcare industry in the area of cybersecurity are discussed below [14]:

- Healthcare industry is facing lack of expert security professionals.
- The legacy equipment is either old or unsupported and contains vulnerable operating systems. The funding dearth allows unsupported equipment to continue functioning.
- The network design is focused heavily on hyper connectivity with less focus on security [32]
- The patient care outage incidents such as locking by ransomware are serious threats to healthcare industry [11]
- Unwillingness to address known vulnerabilities [42]

10.5.3.2 Healthcare Cybersecurity Objectives

The health care security objectives for different patient safety aspects are [1, 22, 35, 66]:

- Confidentiality. The protection of patient information from unauthorized disclosure and access [60].
- Integrity. The protection of patient safety from unauthorized modification of the adequate use of the medical device [102]. It includes the unauthorized access and modification of patient identifiable information including protected health data. The safety of patients' systems from malicious unauthentic actuation, protection of patient physiological data modifications to ensure correct functionality of the software (e.g., processing and algorithmic capabilities) particularly in the monitoring and treatment components of the system are of critical importance.
- Availability. Ensuring the availability of patient information and medical equipment to authorized entities on need basis [50]. It includes rapid updates, secure and authenticated patches, and updates to the equipment, and correct usage of the device for the right purpose thus ensuring and maximizing optimum functionality.

Therefore, continuing cybersecurity risk management is important to use secure state-of-the-art technology [108] to safeguard medical devices and their updates [41]. Some potential cases of risks in the connected medical systems are shown in Fig. 10.6.

10.5.4 Smart Meter

A smart meter is used for electricity usage monitoring. It is used to transmit data to service providers using various types of communication links where this information is used for customer billing, load balancing, energy consumption analysis, and price optimization. The cybersecurity threats related to the smart grids and meters include [39, 45, 46, 62, 97, 97, 107]:

- Malicious attack to disconnect utilities service resulting in loss of power [94]
- Coordinated cascading network attacks on grids, using compromised meters [24]
- Theft and break-in planning when the home owner is away based on the analysis of energy usage [55]
- Denial of service attacks where legitimate requests by the utility service provider are rejected [13]
- Data injection attack to produce invalid measurements of energy consumption [5]
- Smart metering privacy compromising attacks and man in the middle attacks [68]

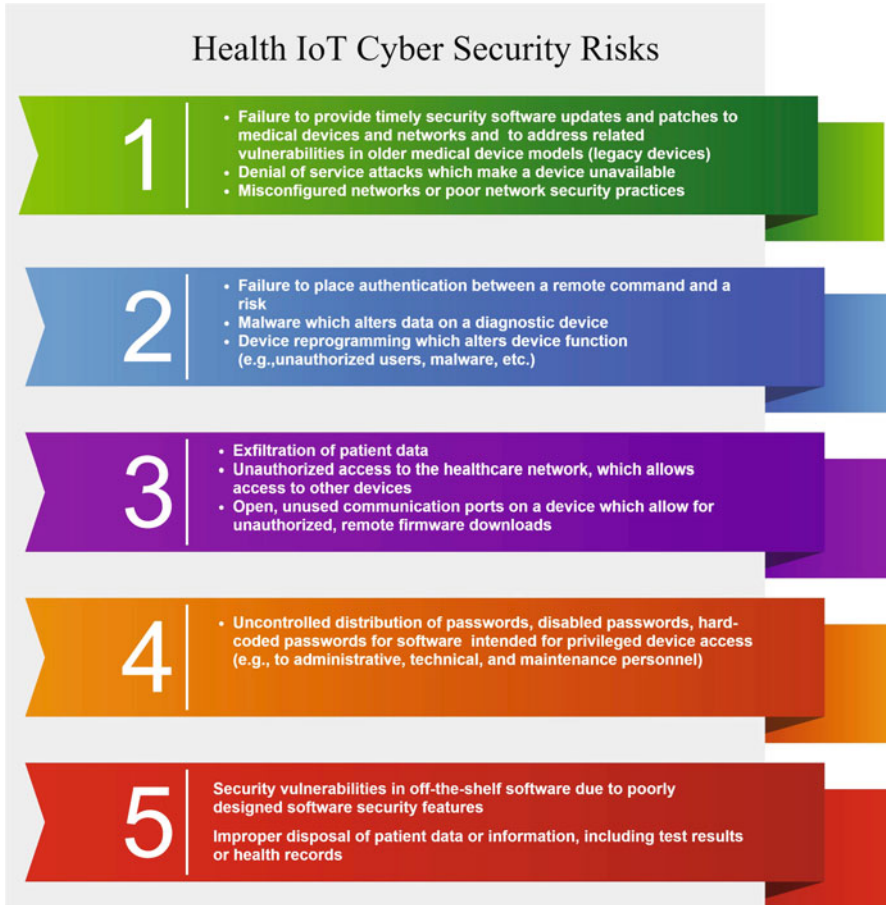


Fig. 10.6 A list of healthcare cybersecurity risks

- The meter spoofing, authentication attacks, and disaggregation attacks are some of the other examples [109]

The smart metering cybersecurity threats are shown in Fig. 10.7.

10.5.5 Water Systems

The fresh water is crucial for life on earth. The water systems face different types of threats such as natural, caused by human activity, disasters, droughts, earthquakes, and terrorism [21, 56, 65].

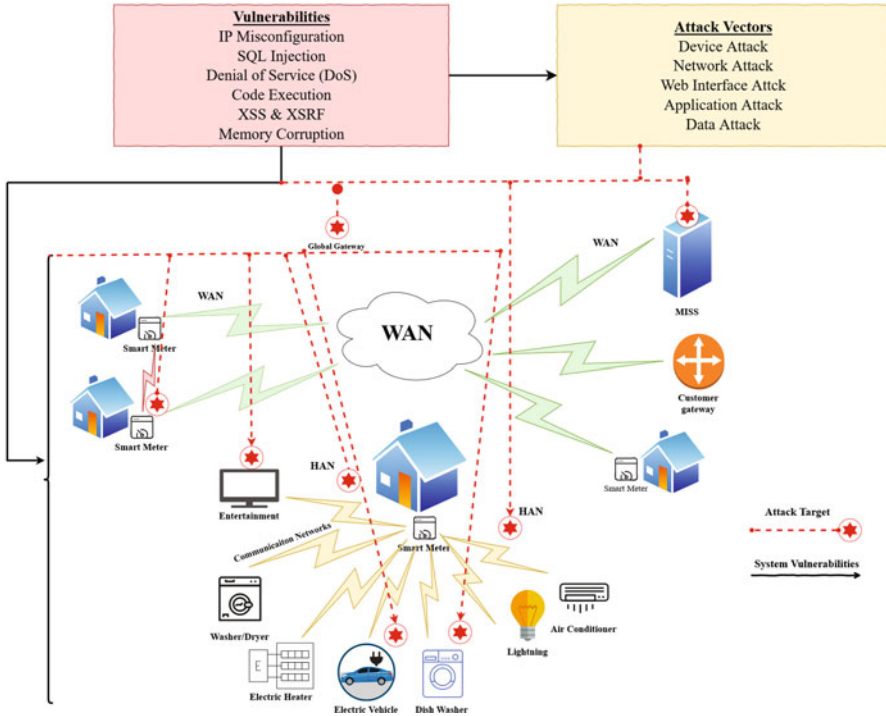


Fig. 10.7 The cybersecurity threats in smart meters [97]

- The contamination attacks and other terrorism related activities, flooding, and storms are the direct threats to these systems [4]
- The water scarcity and lack of water resource availability are also major threats to the sustainability [8]
- Threats of contamination and pollution from point- sources and non-point source and biodiversity loss [48] (see Fig. 10.8.)
- The climate related threats on water [19, 23, 26, 47, 57, 59, 63, 100, 106]

The waters systems security threats can be mitigated by water systems risk characterization, use of sustainable water IoT contamination monitoring and warning systems and through use of advanced machine learning systems for threat modeling [38, 64].



Fig. 10.8 The contamination cycle [99]

References

1. Abraham, C., Chatterjee, D., & Sims, R. R. (2019). Muddling through cybersecurity: Insights from the US healthcare industry. *Business Horizons*, 62, 539–548.
2. Ahmed, E., Yaqoob, I., Gani, A., Imran, M., & Guizani, M. (2016). Internet-of-things-based smart environments: State of the art, taxonomy, and open research challenges. *IEEE Wireless Communications*, 23(5), 10–16.
3. Akyildiz, I. F., & Stuntebeck, E. P. (2006). Wireless underground sensor networks: Research challenges. *Ad Hoc Networks Journal*, 4, 669–686.
4. Andrei, H., Andrei, P. C., Gaiceanu, M., Stanculescu, M., Arama, I. N., & Marinescu, I. (2019). Power systems recovery and restoration encounter with natural disaster and deliberate attacks. In *Power Systems Resilience* (pp. 247–267). Berlin: Springer.
5. Ayad, A., Farag, H. E., Youssef, A., & El-Saadany, E. F. (2018). Detection of false data injection attacks in smart grids using recurrent neural networks. In *2018 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)* (pp. 1–5). Piscataway: IEEE.
6. Barreto, L., & Amaral, A. (2018). Smart farming: Cyber security challenges. In *2018 International Conference on Intelligent Systems (IS)* (pp. 870–876). Piscataway: IEEE.

7. Bell, A. (2019). Applying human viewpoints to risk-based decision-making. In *The Human Viewpoint for System Architectures* (pp. 103–117). Berlin: Springer.
8. Besbes, M., Chahed, J., & Hamdane, A. (2019). On the water security concept: State of the art. In *National Water Security* (pp. 31–55). Berlin: Springer.
9. Bogen, H. R., Herbst, M., Huisman, J. A., Rosenbaum, U., Weuthen, A., & Vereecken, H. (2010). Potential of wireless sensor networks for measuring soil water content variability. *Vadose Zone Journal*, 9(4), 1002–1013.
10. Brass, I., Tanczer, L., Carr, M., Elsdon, M., & Blackstock, J. (2018). Standardising a moving target: The development and evolution of IoT security standards. In *Living in the internet of things: Cybersecurity of the IoT – 2018*. London: IET.
11. Brewczyńska, M., Dunn, S., & Elijah, A. (2019). Data privacy laws response to ransomware attacks: A multi-jurisdictional analysis. In *Regulating New Technologies in Uncertain Times* (pp. 281–305). Berlin: Springer.
12. Burr, W. E. (2003). Selecting the advanced encryption standard. *IEEE Security & Privacy*, 1(2), 43–52.
13. Cameron, C., Patsios, C., Taylor, P. C., & Pourmirza, Z. (2018). Using self-organizing architectures to mitigate the impacts of denial-of-service attacks on voltage control schemes. *IEEE Transactions on Smart Grid*, 10(3), 3010–3019.
14. Care industry cybersecurity task force, H.: Report on improving cybersecurity in the health care industry. <https://www.phe.gov/preparedness/planning/cybertf/documents/report2017.pdf>.
15. Cauteruccio, F., Fortino, G., Guerrieri, A., Liotta, A., Mocanu, D. C., Perra, C., et al. (2019). Short-long term anomaly detection in wireless sensor networks based on machine learning and multi-parameterized edit distance. *Information Fusion*, 52, 13–30.
16. Chatfield, A. T., & Reddick, C. G. (2019). A framework for internet of things-enabled smart government: A case of IoT cybersecurity policies and use cases in US federal government. *Government Information Quarterly*, 36(2), 346–357.
17. Chi, H., Welch, S., Vasserman, E., & Kalaimannan, E. (2017). A framework of cybersecurity approaches in precision agriculture. In *Proceedings of the ICMLG2017 5th International Conference on Management Leadership and Governance* (pp. 90–95). Reading, UK: Acad. Conf. Publ. Int.
18. Childress, R. L., Hagi, S., & Turnham, J. C. (2018). Machine learning statistical methods estimating software system's security analysis assessment or audit effort, cost and processing decisions. US Patent App. 10/095869.
19. Chisolm, E. I., & Matthews, J. C. (2012). Impact of hurricanes and flooding on buried infrastructure. *Leadership and Management in Engineering*, 12(3), 151–156.
20. Coble, K. H., Mishra, A. K., Ferrell, S., & Griffin, T. (2018). Big data in agriculture: A challenge for the future. *Applied Economic Perspectives and Policy*, 40(1), 79–96.
21. Cohen, S. A. (2019). *Cybersecurity for critical infrastructure: Addressing threats and vulnerabilities in Canada* (p. 3340). MSU Graduate Theses. <https://bearworks.missouristate.edu/theses/3340>.
22. Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, 113, 48–52.
23. Davis, C. A. (2014). Water system service categories, post-earthquake interaction, and restoration strategies. *Earthquake Spectra*, 30(4), 1487–1509.
24. Deng, R., Zhuang, P., & Liang, H. (2017). CCPA: Coordinated cyber-physical attacks and countermeasures in smart grid. *IEEE Transactions on Smart Grid*, 8(5), 2420–2430.
25. DHS: Strategic principles for securing the Internet of Things (IoT). https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL.pdf.
26. Dilling, L., Daly, M. E., Kenney, D. A., Klein, R., Miller, K., Ray, A. J., et al. (2019). Drought in urban water systems: Learning lessons for climate adaptive capacity. *Climate Risk Management*, 23, 32–42.

27. Dong, X., Vuran, M. C., & Irmak, S. (2013). Autonomous precision agriculture through integration of wireless underground sensor networks with center pivot irrigation systems. *Ad Hoc Networks*, 11(7), 1975–1987. <http://doi.org/10.1016/j.adhoc.2012.06.012>.
28. Duncan, S. E., Reinhard, R., Williams, R. C., Ramsey, A. F., Thomason, W., Lee, K., et al. (2019). Cyberbiosecurity: A new perspective on protecting us food and agricultural system. *Frontiers in Bioengineering and Biotechnology*, 7, 63.
29. Fagan, M., Megas, K., Scarfone, K., & Smith, M. (2019). Core cybersecurity feature baseline for securable IoT devices: A starting point for IoT device manufacturers. Technical Report, National Institute of Standards and Technology.
30. Ferris, J. L. (2017). Data privacy and protection in the agriculture industry: Is federal regulation necessary. *Minnesota Journal of Law, Science & Technology*, 18, 309.
31. Foege, J. N., Lauritzen, G. D., Tietze, F., & Salge, T. O. (2019). Reconceptualizing the paradox of openness: How solvers navigate sharing-protecting tensions in crowdsourcing. *Research Policy*, 48(6), 1323–1339.
32. Fredette, J., Marom, R., Steiner, K., & Witters, L. (2012). The promise and peril of hyperconnectivity for organizations and societies. *The Global Information Technology Report 2012*, 113–119.
33. Frustaci, M., Pace, P., Aloï, G., & Fortino, G. (2017). Evaluating critical security issues of the IoT world: Present and future challenges. *IEEE Internet of Things Journal*, 5(4), 2483–2495.
34. Gervais, D. (2019). Exploring the interfaces between big data and intellectual property law. *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 10, 3.
35. Ghafur, S., Grass, E., Jennings, N. A., & Darzi, A. (2019). The challenges of cybersecurity in health care: The UK national health service as a case study. *The Lancet Digital Health*, 1(1), e10–e12.
36. Guo, H., & Sun, Z. (2014). Channel and energy modeling for self-contained wireless sensor networks in oil reservoirs. *IEEE Transactions Wireless Communications*, 13(4), 2258–2269. <https://doi.org/10.1109/TWC.2013.031314.130835>.
37. Guo, Z., Shi, D., Johansson, K. H., & Shi, L. (2016). Optimal linear cyber-attack on remote state estimation. *IEEE Transactions on Control of Network Systems*, 4(1), 4–13.
38. Hindy, H., Brosset, D., Bayne, E., Seam, A., & Bellekens, X. (2018). Improving SIEM for critical SCADA water infrastructures using machine learning. In *Computer Security* (pp. 3–19). Berlin: Springer.
39. Hussain, S., Meraj, M., Abughalwa, M., & Shikfa, A. (2018). Smart grid cybersecurity: Standards and technical countermeasures. In *2018 International Conference on Computer and Applications (ICCA)* pp. 136–140. Piscataway: IEEE.
40. Jarmakiewicz, J., Parobczak, K., & Maślanka, K. (2017). Cybersecurity protection for power grid control infrastructures. *International Journal of Critical Infrastructure Protection*, 18, 20–33.
41. Jha, N. K., Raghunathan, A., & Zhang, M. (2018). Securing medical devices through wireless monitoring and anomaly detection. US Patent App. 10/135849.
42. Kapellmann, D., & Washburn, R. (2019). Call to action: Mobilizing community discussion to improve information-sharing about vulnerabilities in industrial control systems and critical infrastructure. In *2019 11th International Conference on Cyber Conflict (CyCon)* (Vol. 900, pp. 1–23). Piscataway: IEEE.
43. Katina, P. F., & Keating, C. B. (2018). Cyber-physical systems governance: A framework for (meta) cybersecurity design. In *Security by Design* (pp. 137–169). Berlin: Springer.
44. Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, 82, 395–411.
45. Khattak, A. M., Khanji, S. I., & Khan, W. A. (2019). Smart meter security: Vulnerabilities, threat impacts, and countermeasures. In *International Conference on Ubiquitous Information Management and Communication* (pp. 554–562). Berlin: Springer.
46. Kimani, K., Oduol, V., & Langat, K. (2019). Cyber security challenges for IoT-based smart grid networks. *International Journal of Critical Infrastructure Protection*, 25, 36–49.

47. Kundzewicz, Z. W., Budhakooncharoen, S., Bronstert, A., Hoff, H., Lettenmaier, D., Menzel, L., et al. (2002). Coping with variability and change: Floods and droughts. In *Natural Resources Forum* (Vol. 26, pp. 263–274). Hoboken: Wiley Online Library.
48. Lankoski, J., & Ollikainen, M. (2013). Innovations in nonpoint source pollution policy – European perspectives. *Choices*, 28(3), 1–5. Cited By 5.
49. Li, F., Li, H., Niu, B., & Chen, J. (2019). Privacy computing: Concept, computing framework, and future development trends. *Engineering*. <https://doi.org/10.1016/j.eng.2019.09.002>.
50. Malik, M. I., Mcateer, L., Hannay, P., & Baig, Z. (2018). Preparing for secure wireless medical environment in 2050: A vision. *IEEE Access*, 6, 25666–25674.
51. Manninen, O. (2018). Cybersecurity in agricultural communication networks : Case dairy farms. Master's thesis, Jyväskylä: JAMK University of Applied Sciences. <https://www.theseus.fi/handle/10024/159476>
52. Markham, A., & Trigoni, N. (2012). Magneto-inductive networked rescue system (miners): Taking sensor networks underground. In *Proceedings of the 11th ICPS, IPSN '12* (pp. 317–328). New York: ACM. <https://doi.org/10.1145/2185677.2185746>.
53. McGettrick, A. (2013). Toward effective cybersecurity education. *IEEE Security & Privacy*, 11(6), 66–68.
54. Mitton, N., Chaouchi, H., Noel, T., Gabillon, T., & Capolsini, P. (2016). Interoperability, safety and security in IoT. In *Second International Conference, InterIoT 2016 and Third International Conference, SaSeIoT*. Berlin: Springer.
55. Molina-Markham, A., Shenoy, P., Fu, K., Cecchet, E., & Irwin, D. (2010). Private memoirs of a smart meter. In *Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building* (pp. 61–66). New York: ACM.
56. Moy de Vitry, M., Schneider, M. Y., Wani, O. F., Manny, L., Leitão, J. P., & Eggimann, S. (2019). Smart urban water systems: What could possibly go wrong? *Environmental Research Letters*, 14(8), 081001.
57. Neiman, P. J., Schick, L. J., Ralph, F. M., Hughes, M., & Wick, G. A. (2011). Flooding in western Washington: The connection to atmospheric rivers. *Journal of Hydrometeorology*, 12(6), 1337–1358.
58. Neshenko, N., Bou-Harb, E., Crichigno, J., Kaddoum, G., & Ghani, N. (2019). Demystifying IoT security: an exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations. *IEEE Communications Surveys & Tutorials*, 21(3), 2702–2733.
59. Peterson, T. C., Heim Jr, R. R., Hirsch, R., Kaiser, D. P., Brooks, H., Diffenbaugh, N. S., et al. (2013). Monitoring and understanding changes in heat waves, cold waves, floods, and droughts in the United States: State of knowledge. *Bulletin of the American Meteorological Society*, 94(6), 821–834.
60. Pirbhulal, S., Samuel, O. W., Wu, W., Sangaiah, A. K., & Li, G. (2019). A joint resource-aware and medical data security framework for wearable healthcare systems. *Future Generation Computer Systems*, 95, 382–391.
61. Prieger, J. E. (2003). The supply side of the digital divide: Is there equal availability in the broadband internet access market? *Economic Inquiry*, 41(2), 346–363.
62. Radhakrishnan, V., Durairaj, D., Balasubramanian, K., & Kamatchi, K. (2019). Development of a novel security scheme using DNA biocryptography for smart meter data communication. In *2019 3rd International Conference on Computing and Communications Technologies (ICCCCT)* (pp. 237–244). Piscataway: IEEE.
63. Ralph, F., Dettinger, M., White, A., Reynolds, D., Cayan, D., Schneider, T., et al. (2011). A vision of future observations for western US extreme precipitation events and flooding: Monitoring, prediction and climate. Report to the Western States Water Council, Idaho Falls.
64. Ramotsoela, D. T., Hancke, G. P., & Abu-Mahfouz, A. M. (2019). Attack detection in water distribution systems using machine learning. *Human-centric Computing and Information Sciences*, 9(1), 13.
65. Rasekh, A., Hassanzadeh, A., Mulchandani, S., Modi, S., & Banks, M. K. (2016). Smart water networks and cyber security. *Journal of Water Resources Planning and Management*, 142(7), 1–2.

66. Ravi, A. R., & Nair, R. R. (2019). Cybersecurity threats and solutions in the current e-healthcare environment: A situational analysis. *Medico-Legal Update*, 19(2), 141–144.
67. Reidy, K. M. (2019). *Strengthening the cybersecurity of the internet of things*. Gaithersburg: NIST.
68. Romdhane, R. B., Hammami, H., Hamdi, M., & Kim, T. H. (2019). A novel approach for privacy-preserving data aggregation in smart grid. In *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)* (pp. 1060–1066). Piscataway: IEEE.
69. Rotz, S., Duncan, E., Small, M., Botschner, J., Dara, R., Mosby, I., et al. (2019). The politics of digital agricultural technologies: A preliminary review. *Sociologia Ruralis*, 59(2), 203–229.
70. Saeed, N., Alouini, M. S., & Al-Naffouri, T. Y. (2019). 3d localization for internet of underground things in oil and gas reservoirs. *IEEE Access*, 7, 121769–121780.
71. Saeed, N., Alouini, M., & Al-Naffouri, T. Y. (Fourthquarter 2019). Toward the internet of underground things: A systematic survey. *IEEE Communications Surveys and Tutorials*, 21(4), 3443–3466. <https://doi.org/10.1109/COMST.2019.2934365>.
72. Salam, A. (2018). *Pulses in the sand: Long range and high data rate communication techniques for next generation wireless underground networks*. Lincoln: ETD collection for University of Nebraska (AAI10826112). <http://digitalcommons.unl.edu/dissertations/AAI10826112>.
73. Salam, A. (2019). A comparison of path loss variations in soil using planar and dipole antennas. In *2019 IEEE International Symposium on Antennas and Propagation*. Piscataway: IEEE.
74. Salam, A. (2019). A path loss model for through the soil wireless communications in digital agriculture. In *2019 IEEE International Symposium on Antennas and Propagation*. Piscataway: IEEE.
75. Salam, A. (2019). Subsurface MIMO: A beamforming design in internet of underground things for digital agriculture applications. *Journal of Sensor and Actuator Networks*, 8(3). <https://doi.org/10.3390/jsan8030041>.
76. Salam, A. (2019). Underground environment aware MIMO design using transmit and receive beamforming in internet of underground things. In *2019 International Conference on Internet of Things (ICIOT 2019)*, San Diego.
77. Salam, A. (2019). An underground radio wave propagation prediction model for digital agriculture. *Information*, 10(4). <https://doi.org/10.3390/info10040147>.
78. Salam, A. (2019). Underground soil sensing using subsurface radio wave propagation. In *5th Global workshop on proximal soil sensing*, Columbia.
79. Salam, A., & Karabiyik, U. (2019). A cooperative overlay approach at the physical layer of cognitive radio for digital agriculture. In *Third International Balkan Conference on Communications and Networking 2019 (BalkanCom'19)*. Skopje, Macedonia, the former Yugoslav Republic of.
80. Salam, A., & Shah, S. (2019). Internet of things in smart agriculture: Enabling technologies. In *2019 IEEE 5th World Forum on Internet of Things (WF-IoT) (WF-IoT 2019)*, Limerick.
81. Salam, A., & Shah, S. (2019). Urban underground infrastructure monitoring IoT: The path loss analysis. In *2019 IEEE 5th World Forum on Internet of Things (WF-IoT) (WF-IoT 2019)*, Limerick.
82. Salam, A., & Vuran, M. C. (2017). Smart underground antenna arrays: A soil moisture adaptive beamforming approach. In *Proceedings of IEEE INFOCOM 2017*, Atlanta.
83. Salam, A., & Vuran, M. C. (2017). Wireless underground channel diversity reception with multiple antennas for internet of underground things. In *Proceedings of IEEE ICC 2017*, Paris.
84. Salam, A., & Vuran, M. C. (2018). EM-based wireless underground sensor networks. In S. Pamukcu, L. Cheng (Eds.) *Underground Sensing* (pp. 247–285). Cambridge: Academic Press. <https://doi.org/10.1016/B978-0-12-803139-1.00005-9>.

85. Salam, A., Vuran, M. C., Dong, X., Argyropoulos, C., & Irmak, S. (2019). A theoretical model of underground dipole antennas for communications in internet of underground things. *IEEE Transactions on Antennas and Propagation*, 67(6), 3996–4009.
86. Salam, A., Vuran, M. C., & Irmak, S. (2016). Pulses in the sand: Impulse response analysis of wireless underground channel. In *Proceedings of INFOCOM 2016*, San Francisco.
87. Salam, A., Vuran, M. C., & Irmak, S. (2019). Di-sense: In situ real-time permittivity estimation and soil moisture sensing using wireless underground communications. *Computer Networks*, 151, 31–41. <https://doi.org/10.1016/j.comnet.2019.01.001>.
88. Sales, N., Remédios, O., & Arsenio, A. (2015). Wireless sensor and actuator system for smart irrigation on the cloud. In *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)* (pp. 693–698). Piscataway: IEEE.
89. Sengupta, A., Leesatopornwongsa, T., Ardekani, M. S., & Stuardo, C. A. (2019). Transactions: Where transactions meet the physical world. In *2019 {USENIX} Annual Technical Conference ({USENIX}{ATC} 19)* (pp. 91–106).
90. Shridhar, V. (2019). The India of things: Tata communications' countrywide IoT network aims to improve traffic, manufacturing, and health care. *IEEE Spectrum*, 56(2), 42–47.
91. Spaulding, A. D., & Wolf, J. R. (2018). Cyber-security knowledge and training needs of beginning farmers in Illinois. In *Proceeding 2018 agricultural and applied economics association annual meeting, Washington, D.C., August 5–August 7*.
92. Stankovic, J. A., Le, T., Hendawi, A., & Tian, Y. (2019). Hardware/software security patches for internet of trillions of things. arXiv preprint arXiv:1903.05266.
93. Temel, S., Vuran, M. C., Lunar, M. M., Zhao, Z., Salam, A., Faller, R. K., et al. (2018). Vehicle-to-barrier communication during real-world vehicle crash tests. *Computer Communications*, 127, 172–186. <https://doi.org/10.1016/j.comcom.2018.05.009>.
94. Temple, W. G., Chen, B., & Tippenhauer, N. O. (2013). Delay makes a difference: Smart grid resilience under remote meter disconnect attack. In *2013 IEEE International Conference on Smart Grid Communications (SmartGridComm)* (pp. 462–467). Piscataway: IEEE.
95. Tian, Y., Zhang, N., Lin, Y. H., Wang, X., Ur, B., Guo, X., et al. (2017). SmartAuth: User-centered authorization for the internet of things. In *26th {USENIX} Security Symposium ({USENIX} Security 17)* (pp. 361–378).
96. Tiusanen, M. J. (2013). Soil scouts: Description and performance of single hop wireless underground sensor nodes. *Ad Hoc Networks*, 11(5), 1610–1618. <http://dx.doi.org/10.1016/j.adhoc.2013.02.002>.
97. Tweneboah-Koduah, S., Tsetse, A. K., Azasoo, J., & Endicott-Popovsky, B. (2018). Evaluation of cybersecurity threats on smart metering system. In *Information Technology-New Generations* (pp. 199–207). Berlin: Springer.
98. Upgradability, N.I.S., Patching: Catalog of existing IoT security standards (2017). https://www.ntia.doc.gov/files/ntia/publications/iotsecuritystandardscatalog_draft_09.12.17.pdf.
99. USGCRP. (2016). Impacts of climate change on human health in the United States: A scientific assessment. <http://dx.doi.org/10.7930/J0R49NQX>.
100. Vano, J. A., Miller, K., Dettinger, M. D., Cifelli, R., Curtis, D., Dufour, A., et al. (2019). Hydroclimatic extremes as challenges for the water management community: Lessons from Oroville dam and Hurricane Harvey. *Bulletin of the American Meteorological Society*, 100(1), S9–S14.
101. Vuran, M. C., Salam, A., Wong, R., & Irmak, S. (2018). Internet of underground things in precision agriculture: Architecture and technology aspects. *Ad Hoc Networks*. <https://doi.org/10.1016/j.adhoc.2018.07.017>.
102. Wang, Z., Ma, P., Chi, Y., & Zhang, J. (2018). Medical devices are at risk: Information security on diagnostic imaging system. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (pp. 2309–2311). New York: ACM.
103. West, J. (2018). A prediction model framework for cyber-attacks to precision agriculture technologies. *Journal of Agricultural & Food Information*, 19(4), 307–330.

104. Window, M. (2019). Security in precision agriculture: Vulnerabilities and risks of agricultural systems. Luleå: Luleå University of Technology. Masters' thesis. <http://tu.diva-portal.org/smash/get/diva2:1322203/FULLTEXT02.pdf>.
105. Wiseman, L., Sanderson, J., Zhang, A., Jakku, E. (2019). Farmers and their data: An examination of farmers' reluctance to share their data through the lens of the laws impacting smart farming, *NJAS—Wageningen Journal of Life Sciences*, 90–91, 100301. ISSN 1573-5214. <https://doi.org/10.1016/j.njas.2019.04.007>.
106. Wobus, C., Lawson, M., Mnes, R., Smith, J., & Minich, J (2014). Estimating monetary damages from flooding in the United States under a changing climate. *Journal of Flood Risk Management*, 7(3), 217–229.
107. Zanghi, E., Do Coutto Filho, M. B., & Stacchini de Souza, J. C. (2019). Conceptual framework for blockchain-based metering systems. *Multiagent and Grid Systems*, 15(1), 77–97.
108. Zhang, Y., Gravina, R., Lu, H., Villari, M., & Fortino, G. (2018). Pea: Parallel electrocardiogram-based authentication for smart healthcare systems. *Journal of Network and Computer Applications*, 117, 10–16.
109. Zhang, Y., Wang, J., & Liu, J. Attack identification and correction for PMU GPS spoofing in unbalanced distribution systems. In *IEEE transactions on smart grid*. <https://doi.org/10.1109/TSG.2019.2937554>.
110. Salam A. (2020) Internet of Things for Sustainable Community Development: Introduction and Overview. In: Internet of Things for Sustainable Community Development. Internet of Things (Technology, Communications and Computing). Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-35291-2_1
111. Salam A. (2020) Internet of Things for Environmental Sustainability and Climate Change. In: Internet of Things for Sustainable Community Development. Internet of Things (Technology, Communications and Computing). Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-35291-2_2
112. Salam A. (2020) Internet of Things in Agricultural Innovation and Security. In: Internet of Things for Sustainable Community Development. Internet of Things (Technology, Communications and Computing). Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-35291-2_3
113. Salam A. (2020) Internet of Things for Water Sustainability. In: Internet of Things for Sustainable Community Development. Internet of Things (Technology, Communications and Computing). Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-35291-2_4
114. Salam A. (2020) Internet of Things for Sustainable Forestry. In: Internet of Things for Sustainable Community Development. Internet of Things (Technology, Communications and Computing). Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-35291-2_5
115. Salam A. (2020) Internet of Things in Sustainable Energy Systems. In: Internet of Things for Sustainable Community Development. Internet of Things (Technology, Communications and Computing). Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-35291-2_6
116. Salam A. (2020) Internet of Things for Sustainable Human Health. In: Internet of Things for Sustainable Community Development. Internet of Things (Technology, Communications and Computing). Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-35291-2_7
117. Salam A. (2020) Internet of Things for Sustainable Mining. In: Internet of Things for Sustainable Community Development. Internet of Things (Technology, Communications and Computing). Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-35291-2_8
118. Salam A. (2020) Internet of Things in Water Management and Treatment. In: Internet of Things for Sustainable Community Development. Internet of Things (Technology, Communications and Computing). Springer, Cham. DOI: [10.1007/978-3-030-35291-2_9](https://doi.org/10.1007/978-3-030-35291-2_9)
119. Salam A. (2020) Internet of Things for Sustainability: Perspectives in Privacy, Cybersecurity, and Future Trends. In: Internet of Things for Sustainable Community Development. Internet of Things (Technology, Communications and Computing). Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-35291-2_10
120. Salam, A.; Hoang, A.D.; Meghna, A.; Martin, D.R.; Guzman, G.; Yoon, Y.H.; Carlson, J.; Kramer, J.; Yansi, K.; Kelly, M.; Skvarek, M.; Stankovic, M.; Le, N.D.K.; Wierzbicki, T.; Fan, X. The Future of Emerging IoT Paradigms: Architectures and Technologies. Preprints 2019, 2019120276 (doi: <https://doi.org/10.20944/preprints201912.0276.v1>).
121. A. Konda, A. Rau, M. A. Stoller, J. M. Taylor, A. Salam, G. A. Pribil, C. Argyropoulos, and S. A. Morin, "Soft microreactors for the deposition of conductive metallic traces on planar, embossed, and curved surfaces," *Advanced Functional Materials*, vol. 28, no. 40, p. 1803020. [Online]. Available: <https://onlinelibrary.wiley.com/doi/abs/10.1002/adfm.201803020>

104. A. Salam, M. C. Vuran, and S. Irmak, "Pulses in the sand: Impulse response analysis of wireless underground channel," in *The 35th Annual IEEE International Conference on Computer Communications (INFOCOM 2016)*, San Francisco, USA, Apr. 2016.
105. A. Salam and M. C. Vuran, "Impacts of soil type and moisture on the capacity of multi-carrier modulation in internet of underground things," in *Proc. of the 25th ICCCN 2016*, Waikoloa, Hawaii, USA, Aug 2016.
106. A. Salam, M. C. Vuran, and S. Irmak, "Towards internet of underground things in smart lighting: A statistical model of wireless underground channel," in *Proc. 14th IEEE International Conference on Networking, Sensing and Control (IEEE ICNSC)*, Calabria, Italy, May 2017.
107. A. Salam and M. C. Vuran, "Smart underground antenna arrays: A soil moisture adaptive beamforming approach," in *Proc. IEEE INFOCOM 2017*, Atlanta, USA, May 2017.
108. —, "Wireless underground channel diversity reception with multiple antennas for internet of underground things," in *Proc. IEEE ICC 2017*, Paris, France, May 2017.
109. —, "EM-Based Wireless Underground Sensor Networks," in *Underground Sensing*, S. Pamukcu and L. Cheng, Eds. Academic Press, 2018, pp. 247 – 285.
110. A. Salam, M. C. Vuran, and S. Irmak, "Di-sense: In situ real-time permittivity estimation and soil moisture sensing using wireless underground communications," *Computer Networks*, vol. 151, pp. 31 – 41, 2019. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S1389128618303141>
111. A. Salam and S. Shah, "Urban underground infrastructure monitoring IoT: the path loss analysis," in *2019 IEEE 5th World Forum on Internet of Things (WF-IoT) (WF-IoT 2019)*, Limerick, Ireland, Apr. 2019.
112. A. Salam, "Pulses in the sand: Long range and high data rate communication techniques for next generation wireless underground networks," ETD collection for University of Nebraska - Lincoln, no. AAI10826112, 2018. [Online]. Available: <http://digitalcommons.unl.edu/dissertations/AAI10826112>
113. A. Salam and S. Shah, "Internet of things in smart agriculture: Enabling technologies," in *2019 IEEE 5th World Forum on Internet of Things (WF-IoT) (WF-IoT 2019)*, Limerick, Ireland, Apr. 2019.
114. A. Salam, M. C. Vuran, X. Dong, C. Argyropoulos, and S. Irmak, "A theoretical model of underground dipole antennas for communications in internet of underground things," *IEEE Transactions on Antennas and Propagation*, 2019.
115. A. Salam, "Underground soil sensing using subsurface radio wave propagation," in *5th Global Workshop on Proximal Soil Sensing*, COLUMBIA, MO, May 2019.
116. —, *Underground Environment Aware MIMO Design Using Transmit and Receive Beamforming in Internet of Underground Things*. Cham: Springer International Publishing, 2019, pp. 1–15.
117. A. Salam and U. Karabiyik, "A cooperative overlay approach at the physical layer of cognitive radio for digital agriculture," in *Third International Balkan Conference on Communications and Networking 2019 (BalkanCom'19)*, Skopje, Macedonia, the former Yugoslav Republic of, Jun. 2019.
118. A. Salam, "An underground radio wave propagation prediction model for digital agriculture," *Information*, vol. 10, no. 4, 2019. [Online]. Available: <http://www.mdpi.com/2078-2489/10/4/147>
119. S. Temel, M. C. Vuran, M. M. Lunar, Z. Zhao, A. Salam, R. K. Faller, and C. Stolle, "Vehicle-to-barrier communication during real-world vehicle crash tests," *Computer Communications*, vol. 127, pp. 172 – 186, 2018. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0140366417305224>
120. M. C. Vuran, A. Salam, R. Wong, and S. Irmak, "Internet of underground things: Sensing and communications on the field for precision agriculture," in *2018 IEEE 4th World Forum on Internet of Things (WF-IoT) (WF-IoT 2018)*, Singapore, Feb. 2018.
121. —, "Internet of underground things in precision agriculture: Architecture and technology aspects," *Ad Hoc Networks*, 2018.
122. A. Salam, "A Path Loss Model for Through the Soil Wireless Communications in Digital Agriculture," in *Proc. 2019 IEEE International Symposium on Antennas and Propagation (IEEE APS 2019)*, Atlanta, GA, USA, July 2019.
123. A. Salam, "A Comparison of Path Loss Variations in Soil using Planar and Dipole Antennas," in *Proc. 2019 IEEE International Symposium on Antennas and Propagation (IEEE APS 2019)*, Atlanta, GA, USA, July 2019.
124. Salam A. (2020) *Internet of Things for Sustainable Community Development*. Springer, Cham. DOI: <https://doi.org/10.1007/978-3-030-35291-2>
125. A. Salam, "Design of Subsurface Phased Array Antennas for Digital Agriculture Applications," in *Proc. 2019 IEEE International Symposium on Phased Array Systems and Technology (IEEE Array 2019)*, Waltham, MA, USA, Oct 2019.
126. A. Salam, "Subsurface MIMO: A Beamforming Design in Internet of Underground Things for Digital Agriculture Applications", *J. Sens. Actuator Netw.*, Volume 8, No. 3, August 2019. doi: 10.3390/jsan8030041