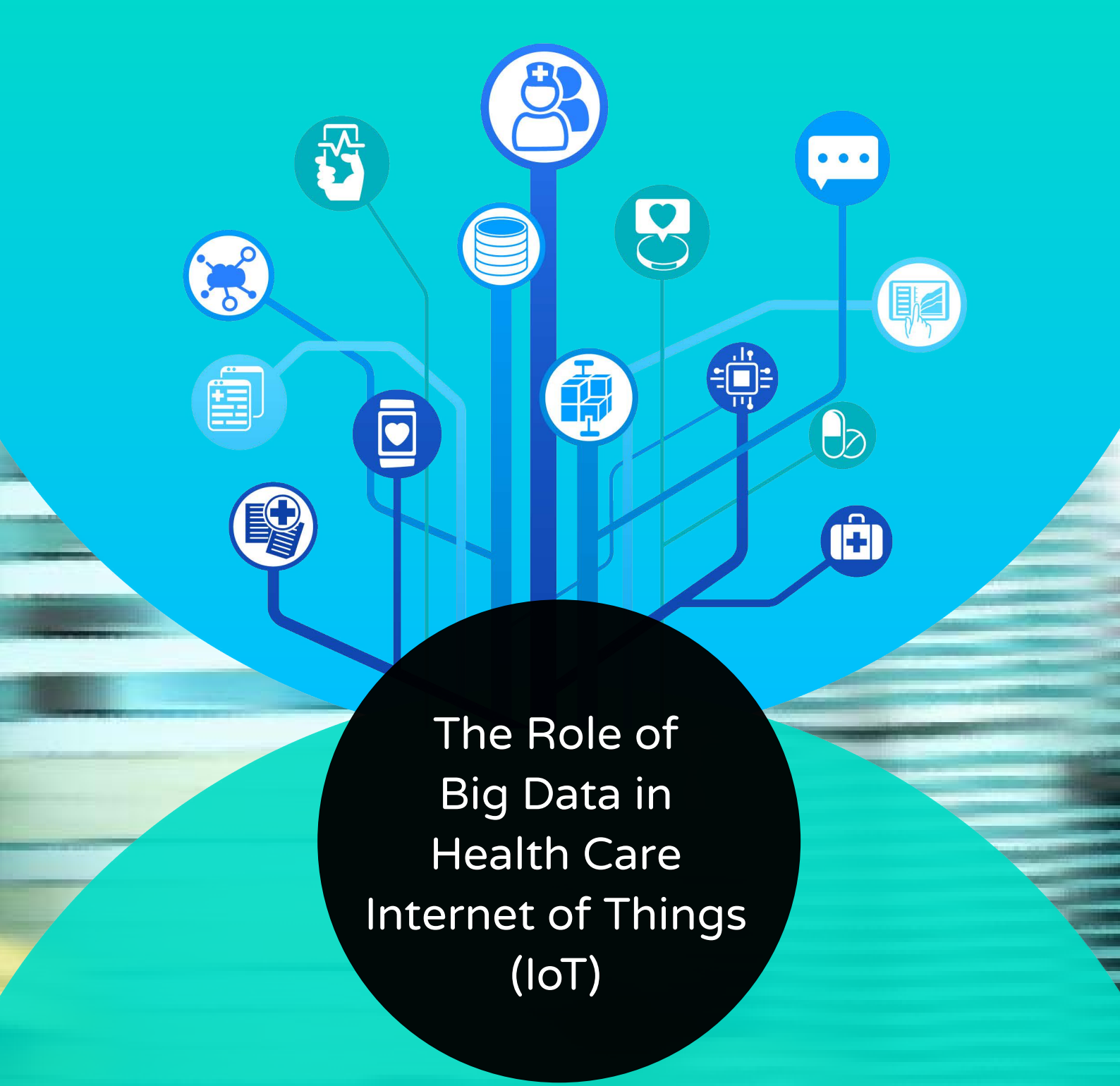


The Role of Big Data in Health Care Internet of Things (IoT)

Technology has been a key part of health care for hundreds, if not thousands, of years. Today, though, the situation is changing. As the Internet of Things (IoT) paradigm becomes more widespread, a host of novel opportunities have arisen. Technologies like miniature wearable biosensors, along with advances in Big Data – especially in regard to efficient handling of large, multiscale, multimodal, distributed and heterogeneous data sets – have opened the floodgates for eHealth and mHealth services that are more personalized and precise than ever before. But the IoT hints at an even greater change in health care paradigms: it promises greater accessibility and availability, personalization and tailored content, and improved returns on investments in delivery.

Even so, as IoT eHealth broadens the horizons of fulfillment in terms of existing health care needs, quite a few major hurdles remain before consistent, suitable, safe, flexible and power-efficient solutions exist to address many medical demands. The only way to cross these hurdles is to facilitate collaboration between the software and hardware sectors, in order to push technology forward. Before a truly IoT-based health care world can emerge, significant advancements in bioelectronics, communication devices, software, and networks, to pattern recognition, sophisticated data-analytics, Big Data and cloud computing, information technologies and media development, along with many areas, still need to take shape.

Health care research brings together a wide range of disciplines and fields, as researchers in medicine, microbiology, biomedical engineering, computer science, and big data analytics frequently find themselves working on related projects. Physicians and microbiologists work together on lab studies and molecular-level diagnostics, in order to maintain or improve patient health. Biomedical engineers use microfluidics and biosensors to engineer new medical tools, and to create novel diagnostic and therapeutic approaches. Computer scientists work to analyze the behaviors of diseases, and algorithmically predict infections based on symptoms, through the use of computer systems and artificial intelligence. Data scientists, meanwhile, conduct pharmaceutical research on cures for diseases like cancer and Ebola, by collaborating with hospitals and clinics to gather data on health care, geolocations, and other related fields.

Considering all these areas of expertise together, it becomes clear that many gaps remain between them; and that these gaps present major technological challenges in the way of the development of a unified, highly adaptive framework for health care. Such a framework, ideally, would correlate alterations in human molecular physiology to the progress, behavior and evolution of specific diseases. In our view, the most direct way to develop this framework is to construct an interactive cyberphysical solution in the form of a cloud-based health care service, in order to facilitate breakthroughs in all areas mentioned above, while enabling more intelligent health care through the use of technologies like smart molecular sensing, therapeutics control, and computational bioinformatics.

Transformational developments in the Internet of Things (IoT)

Advances in the Internet of Things (IoT) help create significant advances in health care. For example, technologies like microfluidic biochips and wearable biosensors can improve clinical diagnostics in a variety of applications, from the laboratory to the hospital. In the foreseeable future, IoT-enabled devices will enable health workers to routinely assess patients who suffer from breast, lung, and colorectal cancers, and perform point-of-care molecular testing as an aspect of standard care. This will help provide physicians with the information they need to create truly data-driven treatment plans, significantly improving the chance of a successful recovery. When these repeated tests are timestamped, location-tagged, and also tagged with data on the testing environment and other situational information, as well as personal information such as age, weight, height and gender, a data fabric will begin to take shape, spotlighting not only the patient's condition, but also overall patterns in the population as a whole (for example, helping predict an outbreak of an epidemic). In short, IoT-enabled health care (eHealth) can move disease research forward, enable more accurate diagnoses at the point of care, and speed up the development of beneficial pharmaceuticals.

We propose the following structure for such an eHealth system:

* eHealth will dynamically process queries about patients at the genomic (e.g., DNA methylation profile), cellular (e.g., blood cells), and organ levels (e.g., kidney activity), across a wide array of wearable, microfluidic biosensors. This system will enable an even greater number of IoT-enabled collaborative experiments to take place in real time, as more labs and researchers collaborate to share data, provide mutual guidance, and leverage this shared database to inform judgments on followup practices and procedures in the biochemical realm.

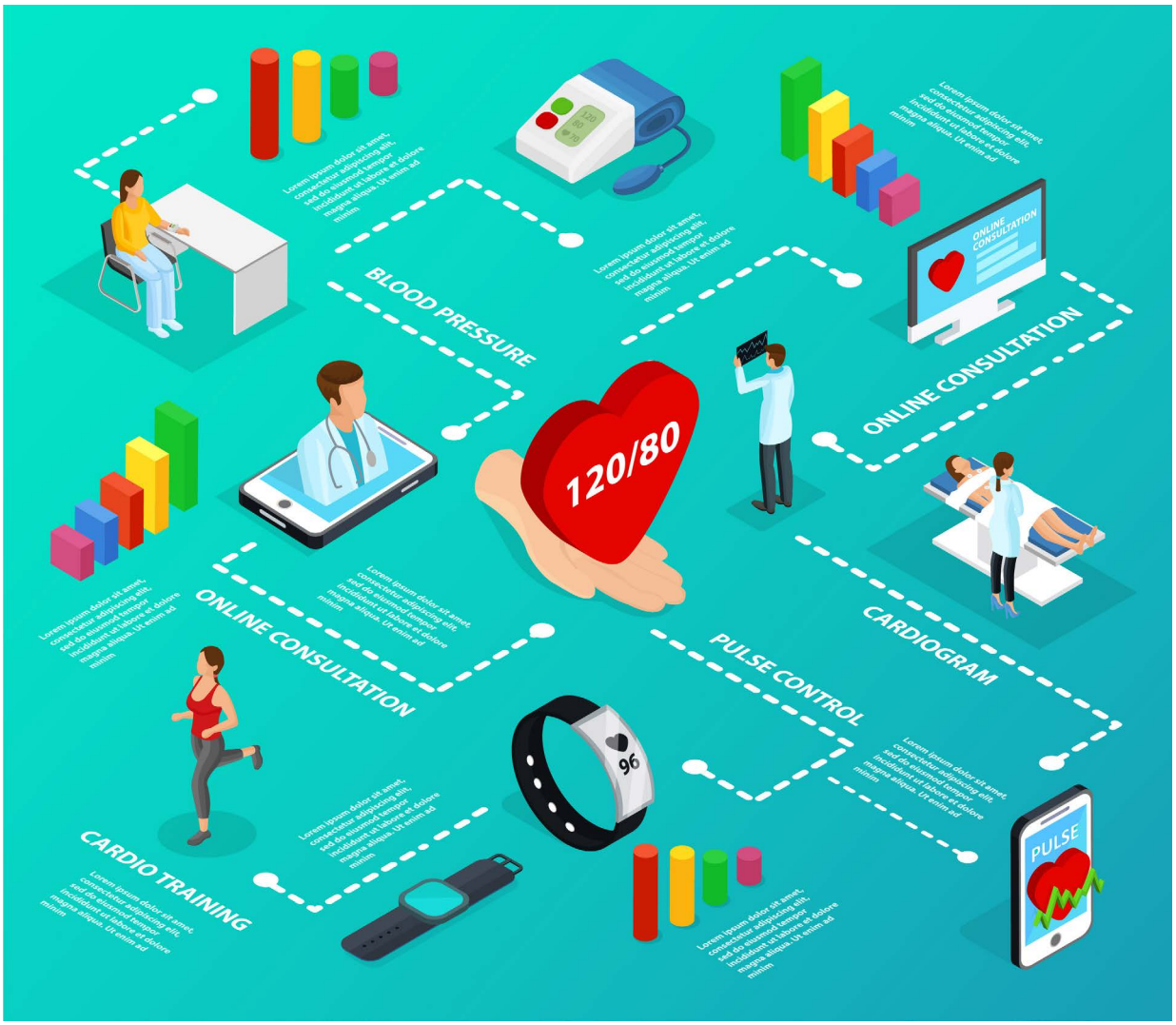
* eHealth will cumulatively develop and improve the accuracy of health care decision making, by utilizing big-data infrastructure to construct genomic-based patient models, through the use of efficient deployments of real-time pattern recognition techniques.

* eHealth will roll out a physical-aware (self-adaptive) health care solution, which joins cyberphysical integration with big-data infrastructure, and can reconfigure its nodes (i.e., modify the properties of implantable devices used to administer specialized medical therapies) in response to dynamically restructuring computational models, which can be tailored by human intervention of self-driven learning. This arrangement will streamline the coupling of patient-related health care data with personalized treatment, and facilitate the ability of thousands of nodes to correlate among themselves.

Health IT needs an innovative interdisciplinary approach

Although electronics have remained the primary focus of EDA, this is nonetheless one of the first engineering disciplines that has emphasized an interdisciplinary approach. The work of chemists, device physicists, electrical engineers, computer scientists, applied mathematicians, operations researchers, and optimization experts has influenced on its abstractions, computational models, algorithms, methodologies, and tools. In fact, many EDA tools can synthesize, optimize, simulae and verify data across all levels of a given abstraction, automatically transforming a complex system-on-chip design from a high-level functional description to a detailed geometric one.

In the health care sector, IoT eHealth faces many of the same data management challenges as in other fields. One distinguishing factor, however, is the fact that



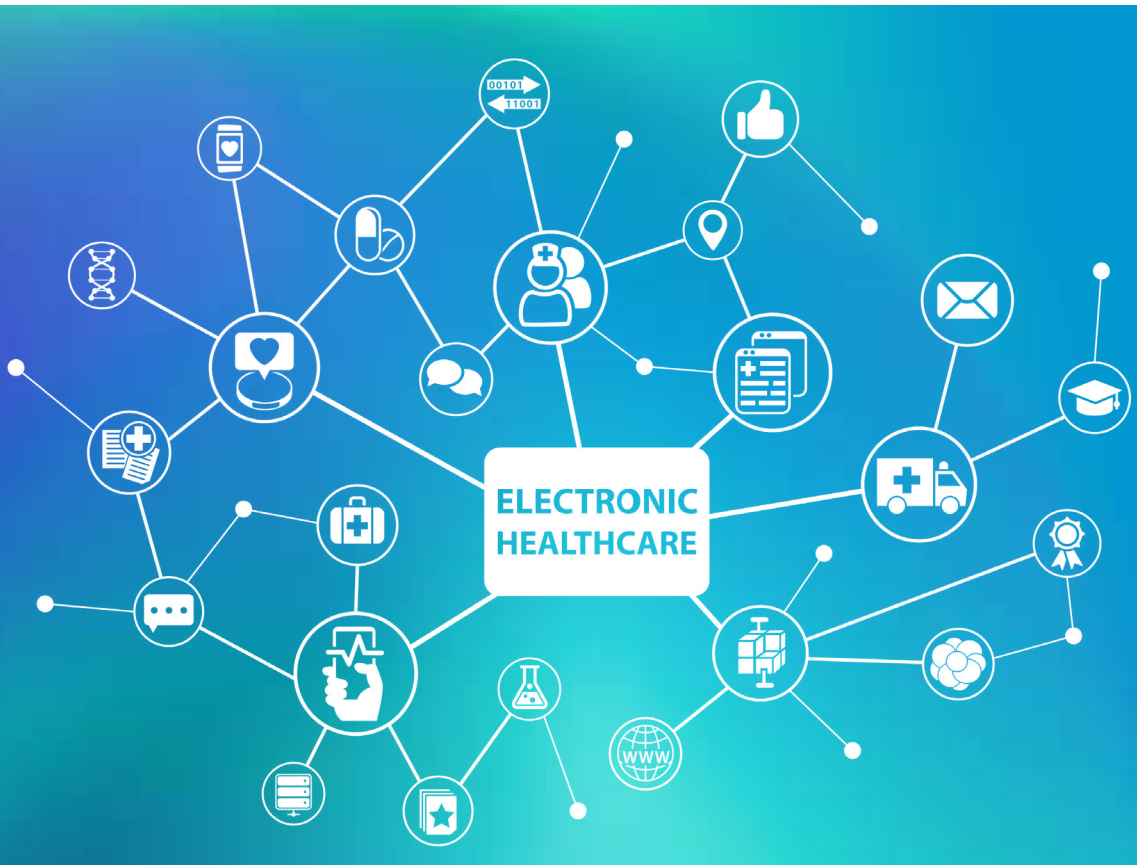
eHealth data originate from medical sensors worn by human subjects; and the human body is a constantly changing system. Thus, from an IoT eHealth perspective, an ongoing flux of data will continually flow inward from edge sensors via fog computing nodes. On a positive note, sensors and computing are both declining in cost, making big data more cost-effective to collect in a brief timeframe. IoT eHeath has evolved to deal with the complicated nature of these data, even as their variety, volume and velocity have continued to increase. At the same time, IoT faces a challenge almost unknown 10 years ago: that of data variety. Dozens of health care applications targeted at end users use their own data format; for example, ECG data is often encoded in XML, while camera-based IoT devices typically record data in a variety of image formats.

Meanwhile, various edge computer manufacturers use their own data formats, which can also vary by customer. Data models on the cloud also vary widely, creating a desperate need for standardization. Difficulties related to data volume and velocity, on the other hand, are more related to the fog node hardware's ability to acquire, analyze, store and transmit data from medical devices (which

could be located at hospitals or clinics, or carried with the patient) at high fidelity and resolution. This creates a clear demand for fog admins capable of supervising the data flux between computing in the cloud and fog.

In order to engineer a health care IoT on a smaller scale, all users will need to have direct access to medical services from portable devices like smartphones, which will need their own sensors specialized for data gathering; along with secure central servers for handling users' requests. Such an arrangement could also be scaled up to the size of a whole hospital, enabling patients throughout he facility to use their mobile devices to get updates on their care, monitor their status, and utilize other medical services. In fact, the model could be scaled up even further, to the scale of an entire city, provided that sensors and antennae exist to collect the needed data, smart algorithms and APIs exist to process it (and to analyze users' requests) and intelligent interfaces exist to pass along real-time information on the statuses of users' requests.

In such a smart city, enabled for eHealth, smartphones would handle all the collection, processing and analysis of data through the use of apps, which would also gather and display feedback on patients' health status, as well as the results of medical checks. This would save tremendous time otherwise spent waiting for appointments and results, and give patients direct access to relevant medical resources, and raise efficiency; all while strengthening trust between patients and their health care providers.



The long-term picture for health IT

The ultimate goal of IoT eHealth is to develop a network of billions of interconnected sensors throughout hospitals, homes, nursing homes, offices and a variety of other locations. Novel routing protocols and network architectures for fog computing nodes will be required in order for the networking sector to rise to this challenge...

Interoperability, standardization and regulatory affairs

The prospect of standardization raises a number of concerns for the IoT. End users, service providers and manufacturers all desire operability both within individual IoT domains, and among them. This creates complex difficulties, however, because the range of disciplines captured by IoT are regulated by a diverse group of regulatory agencies. This complexity is magnified still further in the field of IoT eHealth, where medical standards necessitate particularly strict regulations. In the USE, for insance, wireless medical devices are standardized and regulated by no less than three agencies:

I) the Food and Drug Administration (FDA),
II) the Centers for Medicare and Medicaid Services (CMS), and
III) the Federal Communications Commission (FCC).

Companies who aim to develop IoT applications in the medical area must consider the rules and guidelines of all three of these regulatory bodies. In fact, IoT eHealth's path to market will pass through a complicated multi-agency regulatory environment in the US, as well as in other areas of the globe. IoT eHealth marketed products fall into the category of wellness monitors, which the FDA classifies as low-risk devices, and thus does not regulate as strictly as many other types of medical technology.

Interfaces and human-factor engineering

The interface between front-end technologies like sensors, computers, tablets and other mobile devices provides one of the most immediate challenges for IoT eHealth development. End users (many of whom have little or no knowledge of wireless networking, sensor syncing and similar operations) will be required to self-train in order to use the the devices correctly. In addition, many of the devices will be deployed in remote locations; and elderly populations in particular will be some of the most significant IoT users, highlighting a clear need for eHealth systems that can

be deployed simply and autonomously. Expert involvement will need to be minimized through the use of patient-friendly interfaces. One possible approach is to utilize participatory design, and involve stakeholders and/or end users in the feedback process, in order to make the devices more comfortable and enjoyable to use.

Security and privacy

IoT eHealth devices, like all networked devices, will present some level of potential risk to end users' security and privacy, through the use of unauthorized authentications. This is an especially significant concern in the area of health care, where personal safety could be put at risk. In fact, the entire lifecycle of IoT eHealth is built around privacy and security, from specification generation all the way to implementation and deployment. Even so, a holistic multi-layered set of tactics will be necessary in order to overcome the complex security challenges of engineering an IoT health care ecosystem. This approach is as follows:

Device layer

Connected devices such as sensors, medical devices, gateways, fog nodes, and mobile devices, when involved in capturing, aggregating, processing and transferring medical data to the cloud. Widespread forms of attacks in the device layer include cloning, spoofing, RF jamming, cloud polling and direct connection. In a cloud polling attack, network traffic is redirected in order to inject commands directly to a device, through the use of Man-in-the-Middle (MITM) attacks as well as changes to domain name system (DNS) configuration. The most effective defense against this attack is an ongoing policy of evaluation and verification of certifications, at the device level, in order to ensure that every certificate actually belongs to the eHealth cloud. A direct connection attack, meanwhile, involves the use of a Service Discovery Protocol like Universal Plug and Play (SSDP/UPNP), or the onboard properties of BLE, to locate and target IoT devices. This type of attack is best prevented by a policy of ignoring and blocking unauthenticated requests at the device level, through the use of robust cryptographic algorithms, along with a key management system. Other device-layer security measures include identity, authentication, and authorization management, secure booting (i.e., prevent unauthorized applications to be executed), application sandboxing, whitelisting, fine-grained access control capability of resources, protection of data during capture, storage, and transit, traffic filtering feature, fault tolerance, password enforcement policies, secure

pairing protocols, and secure transmission mechanisms. The extremely limited memory, processing capabilities, power resource, network range, embedded operating systems, thin embedded network protocol stacks of many devices are also vital to take into account when implementing security algorithms in an IoT Health system.

Network layer

In this layer, a whirlwind of diverse network protocols, including Wi-Fi, BLE and ZigBee, are leveraged to establish appropriate connections among sensors. Eavesdropping, Sybil attacks, Sinkhole attacks, Sleep Deprivation attacks, and Man-in-the-Middle attacks are all typical at this level. Thus, the use of trusted routing mechanisms is crucial, as is the use of message integrity verification techniques (using hashing mechanisms like MD5 and SHA) and point-to-point encryption techniques based on cryptographic algorithms. These algorithms fall broadly into two groups: symmetric algorithms such as AES, DES, Blowfish, and Skipjack; and asymmetric public-key algorithms such as Rabin's Scheme, NtruEncrypt and Elliptic Curve Cryptography. As a rule, symmetric algorithms are less computationally intensive, making them more ideal for low-power 8-bit/16-bit IoT devices. At the same time, problematic key exchange mechanisms and confidentiality issues often create difficulties.

Cloud layer

A large body of literature exists on approaches to security issues involved in the deployment of cloud applications; and any company aiming to provide eHealth products and services will need to establish an efficient, effective set of tactics for proactively combating negative impacts of attacks. Widespread vulnerabilities in the cloud include Denial-of-service (DoS) attacks, SQL injections, malicious code injections, Spear-Phishing attacks, sniffing attacks, path traversals, unrestricted file uploading (remote code execution), cross-site scripting (XSS), Trojan horses, viruses, and brute-force attacks using weak password recovery methods.

Human layer

The fundamental principle of IoT eHealth security is that individuals should receive training on how and when to avoid disclosing private health care information. If a knowledgeable group of attackers gains physical access to an end user's IoT eHealth device, those attackers could directly pull data from the device's internal memory and firmware, and modify its settings

to obtain partial or complete control over it. In addition, it will be crucial to train users to avoid such common security pitfalls as sharing physical or electronic keys, choosing weak passwords (such as "1234"), or purchasing used medical equipment.

Even so, one key question remains: how can we utilize the research approaches and concepts of EDA for design automation (DA) in new domains that are now emerging, in order to solve concrete and critical problems of the modern world?

The problems that stand most to benefit from the application of EDA approaches are no longer to be found on a silicon chip, but in the large-scale issues faced by human society on the whole.