A Blockchain Platform in Connected Medical-Device Environments

Trustworthy technology to guard against cyberthreats.

By Ioannis Paliokas, Nikolaos Tsoniotis, Konstantinos Votis, and Dimitrios Tzovaras

©ISTOCKPHOTO.COM/TEEKID

For consumer-oriented medical devices, the issues of rising cybersecurity threats and the need of end users to maintain control lead to a search for effective solutions. This article presents a blockchain framework for consumer-oriented medical devices aiming at added value, including immutability, auditability, and accountability in processes such as user-device binding, registration, maintenance, and alerting. The proposed solution implements a set of smart contracts (SC) to deliver more secure services in smart-home environments.

RISING THREATS

Consumer-oriented medical devices, which are increasingly integrated with smart homes, represent a possible target for cyberattackers. Invasive medical devices, such as pacemakers, and consumer-oriented medical devices, including insulin pumps, digital thermometers, and wearables, continuously become more complex and exposed to cybersecurity threats as well as challenges in authentication, maintenance, alert management, and control. Although each type of attack differs in its behavior, and the methods to prevent or recover from it, some generic threats to medical devices [1] include disruption of device

Digital Object Identifier 10.1109/MCE.2019.2905516
Date of publication: 11 June 2019

2162-2248/19©2019IEEE

communications, database injection, data replaying, spoofing, phishing, denial of service, destruction, and privileges escalation.

There are medical devices that are consumer-grade electronics for private use and that connect to the Internet of Things. Garge et al. used the term "consumer healthcare" [2] to describe various aspects of care that can benefit from consumer-grade health-monitoring devices. Silva et al. [3] presented an approach to integrate medical devices with interactive digital TV technology by means of software running into one residential gateway and mobile devices. Others have proposed portable solutions for patient monitoring (biomedical signal processing) [4] and the use of smartphones to offer additional processing power [5]. To address these issues, we envision a transparent cybersecurity environment for consumer-oriented medical devices based on blockchain technology.

STATE OF THE ART

Though smart solutions help to provide quality health care, they also become vulnerable to threats [6]. The vulnerability grows with the increase in usage and connectivity. In most devices, security aspects tend to be minimal because of a lack of focus on security in embedded systems, which presents major vulnerabilities due to: 1) lack of specialized software, 2) low ability of the equipment to integrate security, and 3) outdated network security.

Modern medical devices deal with sensitive data that refer to either personally identifiable user information or critical parameters of device control. Both should be considered for protection from malicious attacks, but existing network-security solutions only have a limited effect on the cybersecurity defense of connected medical devices. Authentication using biometrics is another option, but people are generally suspicious of this alternative [7], and, especially in home environments, those misgivings can be sufficient to lead to failure. In parallel, a number of organizations [for example, the U.S. Food and Drug Administration (FDA) and the International Organization for Standardization] are contributing to the elaboration of standards (for example, X.1120 and X.1139) [8]. Fortunately, there are standards for software-lifecycle processes (such as EN 62304:2006) and the National Institute of Standards and Technology's FDA-recommended cybersecurity framework as well.

The Hyperledger was initiated as an open source project to support the collaborative development of blockchain-distributed ledgers. Similarly, the Coco Framework enables high-scale blockchain networks for enterprises. There is expressed concern about personal-data regulations, especially about the "right to erasure." Storing personal data in the blockchain could be a breach of privacy regulations (for example, Europe's General Data Protection Regulation). This becomes very important, especially when having to do with medical data, such as in the case of the MedRec Blockchain

Modern medical devices deal with sensitive data that refer to either personally identifiable user information or critical parameters of device control.

[9]. Blockchain technology has been used to provide electronic health records with better immutability, cybersecurity, and interoperability [10]. However, to the data regulators and policy makers, cryptography is an acceptable solution.

Among others, the energy-consumption behavior is a key factor to identify abnormal applications in mobile devices [11] with resource constraints [12], including medical devices. For the latter, there are algorithms, such as the battery-performance alert, that can identify deviations from normal battery performance with a high degree of sensitivity by analyzing the daily battery voltage [13]. Additionally, attack-detection algorithms (for instance, seed expanding) can recognize an attack before it causes any damage to the system [14].

THE PROPOSED SOLUTION

The main challenge in smart home environments with interconnected medical devices is the incorporation of human behavior into those systems [15]. Armor chain proposes an increasingly fundamental role for a number of novel technologies that can drastically contribute to both medical-device cybersecurity and the human-behavior incorporation inside consortia. Members of those communities need to know:

- "Are you the manufacturer you say you are?"
- "Are you the consumer who makes use of this device?"
- "Should you have permission to perform an update/fix to this device?"

These questions can be answered by the proposed architecture by using blockchain over the existing security layer, if any.

Armor-chain architecture is targeted mainly at specific types of cyberthreats and vulnerabilities related to the questions in the previous paragraph, including inadequate authentication mechanisms, unauthorized access to medical devices, and cyberattacks to steal medical-data records. Other types, such as phishing attempts, man-in-the-middle, and replay attacks, are taken into consideration (although they are not very possible due to secure EIP155 transaction types and the fact that the private keys are kept safe) as well as prevention against malware infection, such as viruses, worms, and so forth. Other malicious software, including rootkits and botnets, are considered to be infrequent types of attacks on medical devices.

THE BLOCKCHAIN IN CONNECTED MEDICAL DEVICES

The blockchain employed is a semiprivate Ethereum-based network. This technology was chosen because of the flexibility of its SC and the fact that it uses a virtual machine built

Consumer-oriented medical devices, which are increasingly integrated with smart homes, represent a possible target for cyberattackers.

on top of it. An *SC* is a computer code maintained on the nodes of the blockchain that is capable of making an agreement under certain predefined conditions. Other characteristics derived from the Ethereum-based network include:

- *Control and confidence*: Consumers have greater control over medical-device installation and operation in smart-home environments (consumer-manufacturer binding).
- *Maintainability*: There is critical system-protection technology and increased software maintainability for medical devices that have some processing power. Depending on processing/storage capacity, devices are able to embed cybersecurity features, share threat intelligence at the community level, and introduce a coordinated risk-based approach.
- *Risk monitoring and assessment*: There is proactive real-time risk assessment (by creating and maintaining a risk register), anomaly detection, big-data analytics, and advanced visualization tools. The main elements of this are 1) a lightweight software agent for threat monitoring assisted by an artificial-intelligence component and 2) a dynamic real-time cyberthreat-intelligence repository (available to all manufacturers in the ecosystem).
- *Blockchain properties*: The network provides immutability (data stored cannot be changed), accountability (users of timestamped services can reliably verify the expected service operation), and auditability (the ability to access a full security audit).

Armor chain provides a cybersecurity framework (Figure 1), implemented as a vendor neutral and protocol-agnostic configuration, to ensure interoperability with multiple devices and to remove relevant barriers. Under it, customers make use of their own computational resources on a peer-to-peer basis. The proposed architecture primarily serves the needs of patients and device manufacturers. This would be made possible by using three types of SCs. The manufacturer SC contains a map used to link devices through its media-access control (MAC) address to a unique device SC address. This contract, owned by the medical device manufacturer, would be updated when a device SC was deployed. The latter contains a subset of the device attributes, such as the MAC address, the QR code, the Ethereum address of the manufacturer, and the gateway smart contract address. Only the manufacturer and the consumer are allowed to modify this SC. Moreover, this SC is enhanced by functions that notifies users about the requests made by the manufacturer and the status of the device.

The gateway SC would be owned by the user and contain the functionality required to create a new device SC. In the case of an SC at device registration, the data in the rest of the blocks cannot be changed without a similar alteration in all subsequent blocks. A collusion of the network majority is required for such a change, and this is what creates an added value to the system. Authorizing transactions comes as the result of the entire armor-chain network. Anonymization is applied between customers and the data saved in the blockchain. The identity of the public-key owner is not easy to find. But, even in such cases, the expected sequence is: person → anonymization → public key → data → blockchain. There is

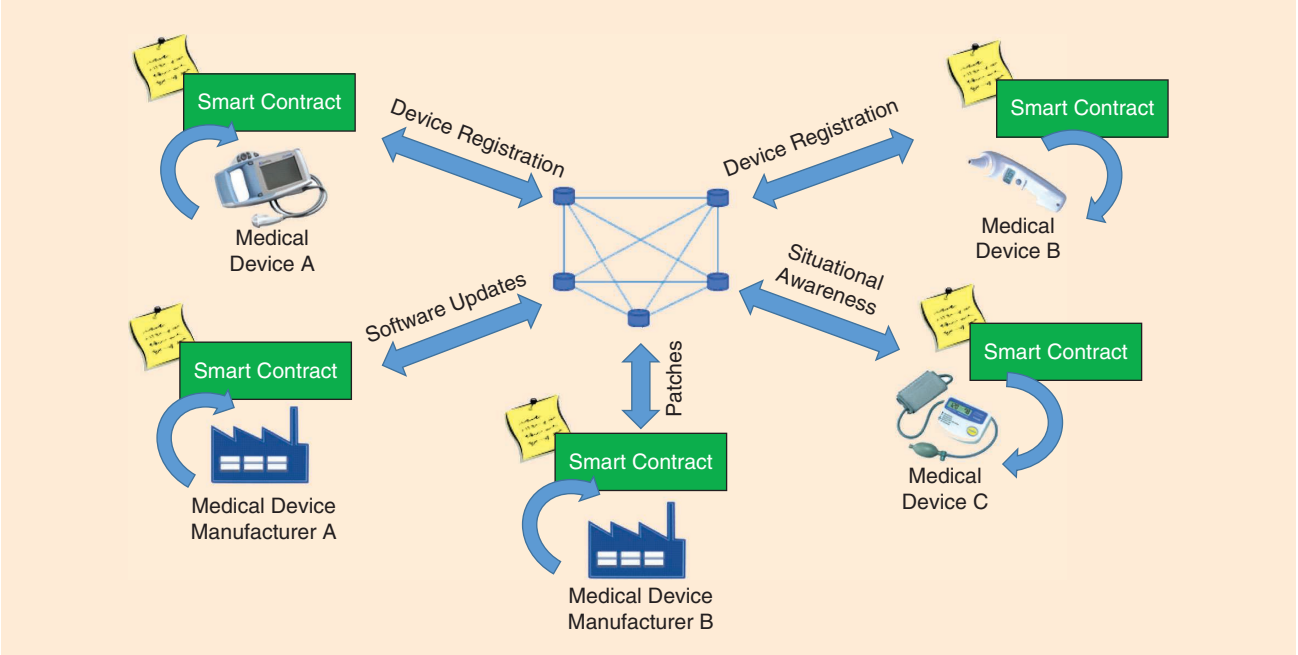

FIGURE 1. The armor-chain conceptual architecture.

no need to store information about who owns the anonymity token inside the blockchain (it is stored outside). Upon a catastrophic incident striking the anonymity token, there will be no forward impact onto the armor chain. The sensitive data related to the medical-apparatus operation are not saved in the blockchain but in the appliance, a mobile device (in the case of coupled devices), external media, or the gateway memory.

From the consumer/patient point of view, the proposed architecture provides solutions for 1) medical-device registration, 2) maintenance, and 3) management of notifications. Keystores are downloaded by users upon registration (light nodes) and stored in their respective node implementation. Regarding the registration of the medical device to the gateway of the smart home, the gateway's interface is used to enter the appliance data and the user's Ethereum address. Registration of a new device with the gateway is allowed only for users whose Ethereum addresses were registered with a gateway contract.

After registration, the manufacturer SC contains links between the device MAC address and its SC address. For maintenance, updates to medical devices registered to the manufacturer SC can be performed. This SC triggers the methods of the device SC, which sends a notification to ask the user for permission to proceed with diagnostics, software updates, and patch installations. It should be noted that only the owner of the device can see and respond to this notification, as long as he or she is the only person who has access to the device SC. In the case of a positive response, access to the medical device is enabled via the gateway, and the manufacturer proceeds with updates. Before closing this maintenance circle, and after a successful update/patch, the device SC will update the blockchain, and access to the medical appliance will be restricted again.

> The main challenge in smart home environments with interconnected medical devices is the incorporation of human behavior into those systems.

ARMOR-CHAIN SYSTEM

In the armor-chain architecture (Figure 2), users are connected in the network as "light nodes" that download only the block headers, and they verify the proof-of-work (PoW) only on them. Users are not miners who participate in the PoW consensus algorithms (which is much less costly in terms of memory, storage, and computational power). Mining takes place through the device manufacturer's nodes and the gateways' nodes. Speed, though a possible issue at this stage, where Ethereum networks are based on PoW, will be greatly improved in the near future when proof-of-stake is applied.

The situational-awareness component is responsible for monitoring the network activity of the supervised medical devices, and it is the part that interfaces between the overall system elements and the physical world (for example, users and manufacturers). The gateway blockchain nodes lie within this component. The coordinated-response component collects data from the medical devices and their network activity through the gateways, which, coupled with the threat-modeling analysis, are used to inform the medical-device manufacturers of potential alerts and their respective categories. In case network traffic looks suspicious (based on predefined patterns), temporary isolation of the device, or forced diagnostics and a

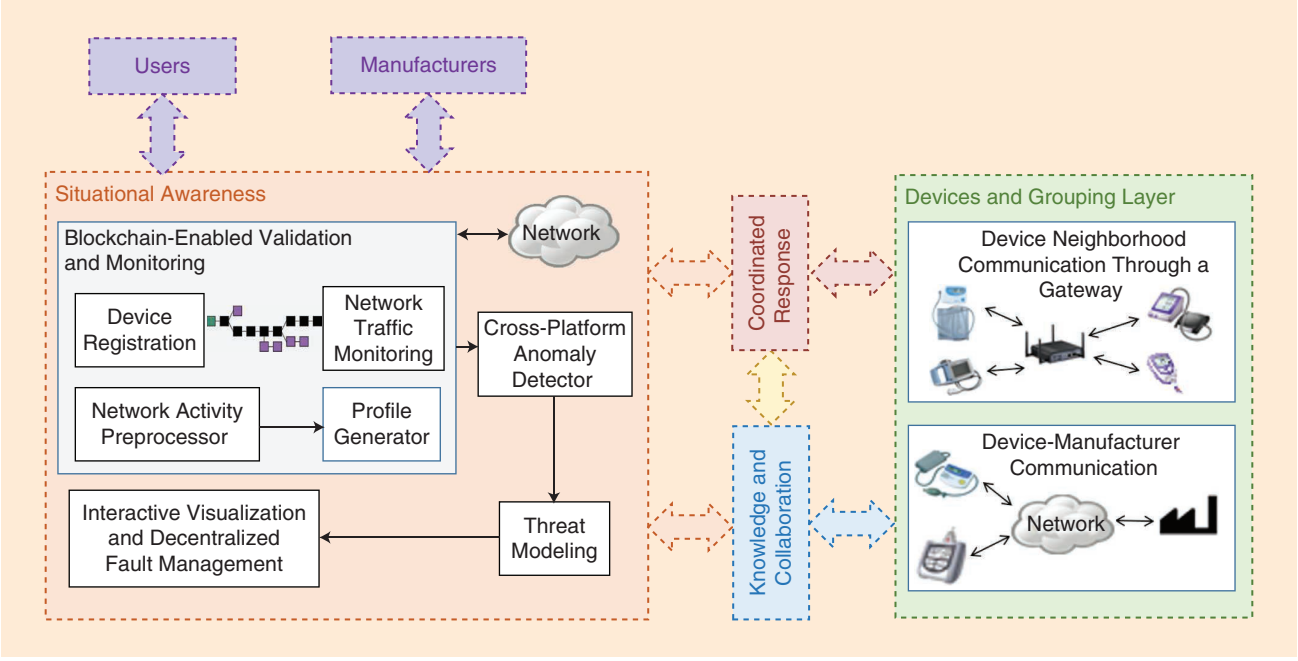

FIGURE 2. The armor-chain system architecture.

fix, will be considered depending on the equipment type and its role.

The knowledge-collaboration component serves as a complete and consolidated record of network activity, tracking, and auditability. The device and grouping layer is responsible for all interconnections of devices within either the local network or the Internet. Nodes in the proposed blockchain approach are the smart-home gateways and the manufacturers. In home environments, gateways are the devices through which all network activity from and to medical equipment is redirected. In addition, smart-home gateways are used as processing units capable of holding the interface used to register devices and serve approval for updates and to run the monitoring and visual analytics. A smartphone can also be used for extra processing power. In more detail, the SCs used in armor chain are as follows.

- *Consumer device (manufacturer)*: While users participate in the blockchain network as light nodes, manufacturers and gateways participate in the mining process to add/verify new transactions to the blockchain, which include all past records. The first SC aims to bind manufacturers, consumers (using their Ethereum address), and medical devices (MAC addresses). Users create new accounts with a keystore and an Ethereum address. During a new medical-device registration, users can employ their smartphones to scan the QR code of the equipment provided by the manufacturer.
- *Maintenance (access rights management)*: A second SC is used for giving access to the manufacturer to regularly update the medical device's software and to send a patch after a risk alert (the manufacturer's response to a cybersecurity threat) as seen in Figure 3. With this SC, users give permission to manufacturers (using their manufacturer's Ethereum address) after receiving a notification. The processing of the request (to accept/reject the update patch as part of the permission-based logic) is conducted through either the gateway's interface or the consumer's mobile application. Note that the notification is visible only to the consumer as he or she has rights to uniquely instigate a change of state to the device SC. Upon acceptance of the notification by the user, the manufacturer sends the update patch on the Internet (through the gateway). After a successful update, access rights to the medical device are revoked by the SC.
- *Situational awareness (risk detection and notifications)*: The third kind of SC is activated after an unusual activity (such as abnormal battery consumption or network traffic) has been detected in a medical device by the software-monitoring component, which is active on the gateway (Figure 4). During an incident, a notification is sent from the manufacturer to the user to ask for urgent permission to access the device to run diagnostics and repairs. The rest of the process is similar to the previous one (maintenance and returning to restricted device access).

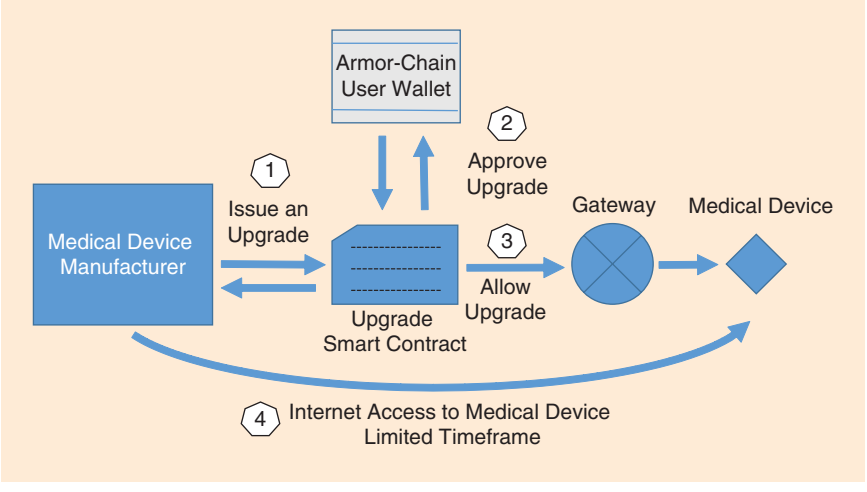

FIGURE 3. The medical-device maintenance process.

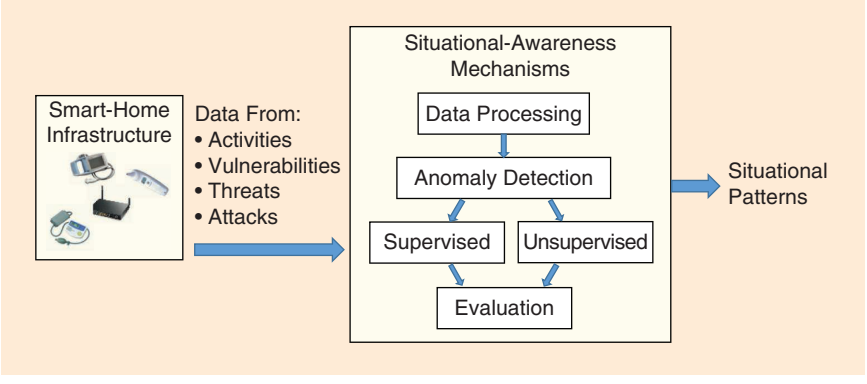

FIGURE 4. The situational-awareness mechanism.

The main sensing process is performed by the blockchain-enabled validation and monitoring element, which is responsible for registering devices and validating all semiprivate network transactions, including messages between devices. The validation of device integration in home environments can be handled by the SCs either as a single device or within neighborhoods of devices. For each undertaking, the block of the transaction will be broadcast to every node of the blockchain-distributed network, and all nodes of the network will approve (validate) the transaction. Afterward, the block is added to the chain for indelible and transparent transactions. Then, the actual message is posted to the targeted device. The node participants (manufacturers) need to obtain an invitation to join, and it is a consortium that makes such decisions. Once entrants join the network, they gain a role in the blockchain maintenance in a decentralized manner.

In general, the alert mechanism that lies behind the situational awareness provides manufacturers and users

access to real-time information from existing armor-chain installations (nodes of the blockchain). A detected cyberattack on a specific medical device triggers automated actions that sends an alert to all other similar devices in the network. Moreover, collaboration enables manufactures to share and access the knowledge base of cybersecurity attacks and enhances the alerts to similar medical devices and their producers. This notification (alerting component) is part of the blockchain, and the real-time notifications will be triggered by the corresponding SCs. Information, such as the device type, timestamp, manufacturer, type of attack, and a number indicating the confidence of the system that an actual attack is occurring, will be circulated.

CONCLUSION

Armor chain is a semiprivate, permissioned, decentralized network. Sensitive data are not saved in the blockchain but in the medical device or external media. Blockchain can combine networking solutions with the security of cryptography to give consortium members a safer way to establish trust. SCs have the ability to implement sophisticated logic. Moreover, starting from zero availability and visibility for devices, an approach that is also followed by software-defined perimeter solutions [16], armor chain always requires verification of users and devices (no default trust) for any party.

Limitations related to Ethereum-based systems include scalability issues due to an inefficient consensus algorithm that may lead to increased time and cost to handle information. In private networks, this problem is not expected to be a blocking issue; however, alternative consensus mechanisms are proposed. Another armor-chain limitation emerges during instances of physically inserted malware (for example, via USB). The resulting abnormal activity may be detected through the armor-chain platform (indirect detection) and, thus, the right SC could be triggered to allow the device manufacturer to run diagnostics. This is in line with experts' advice to use blockchain deployments only after checking their ability to provide a better level of security [17].

Future plans include validating the proposed architecture in a real-life context, simulating cyberattacks, and ensuring overall system-design stability and effectiveness. This includes a technical analysis of the assessment of the data-protection impact to indicate whether the proposed architecture is any better than a traditional cloud-based system.

ABOUT THE AUTHORS

Ioannis Paliokas (ipaliokas@iti.gr) has been a postdoctoral researcher in the Information Technologies Institute at the Center for Research and Technology–Hellas, Thessaloniki, Greece, since 2012.

Nikolaos Tsoniotis (n.tsoniotis@iti.gr) is a research and development engineer and serial entrepreneur in information and communications technology.

Konstantinos Votis (kvotis@iti.gr) is a researcher C in the Information Technologies Institute at the Center for Research and Technology–Hellas, Thessaloniki, Greece, and has been involved in a number of European Community and nationally funded R&D projects.

Dimitrios Tzovaras (tzovaras@iti.gr) is a researcher A in the Information Technologies Institute at the Center for Research and Technology–Hellas, Thessaloniki, Greece, where he has worked since 1999.

REFERENCES

[1] R. Piggin, "Cybersecurity of medical devices: Addressing patient safety and the security of patient health information," BSI Group, Macquarie Park, Australia, White Paper, 2017. [Online]. Available: https://goo.gl/8ao1H8

[2] G. K. Garge, C. Balakrishna, and S. K. Datta, "Consumer healthcare: Current trends in consumer health monitoring," *IEEE Consum. Electron. Mag.*, vol. 7, no. 1, pp. 38–46, 2018. doi: 10.1109/MCE.2017.2743238.

[3] V. J. Da Silva, O. B. Maia, M. Rodriges, and V. F. de Lucena, "Universal system for integrating commercial medical devices with standardized digital TV system," in *Proc. IEEE Int. Conf. Consumer Electronics*, 2016, pp. 301–304.

[4] C. C. Wu, S. H. Fan, S. Chuang, J. J. Liao, C. C. Chou, and W. C. Fang, "A wireless photoplethysmography signal processing system for long-term monitoring," in *Proc. IEEE Int. Conf. Consumer Electronics*, 2016, pp. 480–483.

[5] L. Pepa et al., "Real-time step length estimation on smartphone," in *Proc. IEEE Int. Conf. Consumer Electronics*, 2016, pp. 315–316.

[6] P. Sundaravadivel, E. Kougianos, S. P. Mohanty, and M. Ganapathiraju, "Everything you wanted to know about smart healthcare," *IEEE Consum. Electron. Mag.*, vol. 7, no. 1, pp. 18–28, 2018. doi: 10.1109/MCE.2017.2755378.

[7] P. M. Corcoran, "Biometrics and consumer electronics: A brave new world or the road to dystopia?" *IEEE Consum. Electron. Mag.*, vol. 2, no. 2, pp. 22–33, 2013.

[8] U.S. Food and Drug Administration. (2016). Postmarket management of cybersecurity in medical devices: Guidance for industry and Food and Drug Administration staff. U.S. Food and Drug Administration. Washington, D.C. [Online]. Available: https://goo.gl/5MMuhc

[9] E. Ariel, A. Azaria, J. D. Halamka, and A. Lippman, "A case study for blockchain in healthcare: MedRec prototype for electronic health records and medical research data," Office Nat. Coordinator Health Inform. Technol., Washington, D.C., White Paper, 2016. [Online]. Available: https://goo.gl/de6asr

[10] C. Burniske, E. Vaughn, J. Shelton, and A. Cahana, "How blockchain technology can enhance EHR operability," ARK Investment Management, New York, NY, White Paper, 2016. [Online]. Available: https://goo.gl/DSjAH9

[11] X. Ma et al., "eDoctor: Automatically diagnosing abnormal battery drain issues on smartphones," in *Proc. 10th USENIX Networked Systems Design and Implementation*, 2013, pp. 57–70.

[12] J. Qadri and M. Chen, "A review of significance of energy-consumption anomaly in malware detection in mobile devices," *Int. J. Cyber Situational Awareness*, vol. 1, no. 1, pp. 210–230, Nov. 2016. doi: 10.22619/IJCSA.2016.1001010.

[13] Abbott Laboratories, "Battery performance alert: A tool for improved patient management for devices under battery advisory," Abbot Laboratories, Chicago, IL, 2017. [Online]. Available: https://goo.gl/SEgXr1

[14] J. Wang, L. Yang, J. Wu, and J. H. Abawajy, "Clustering analysis for malicious network traffic," in *Proc. IEEE Int. Conf. Communications*, 2017, pp. 1–6, doi: 10.1109/ICC.2017.7997375.

[15] D. N. Crowley, E. Curry, and J. G. Breslin, "Citizen actuation for smart environments: Evaluating how humans can play a part in smart environments," *IEEE Consum. Electron. Mag.*, vol. 5, no. 3, pp. 90–94, 2016. doi: 10.1109/MCE.2016.2556918.

[16] D. Puthal, S. P. Mohanty, P. Nanda, and U. Choppali, "Building security perimeters to protect network systems against cyber threats," *IEEE Consum. Electron. Mag.*, vol. 6, no. 4, pp. 24–27, 2017.

[17] D. Puthal, N. Malik, and S. P. Mohanty, "The blockchain as a decentralized security framework," *IEEE Consum. Electron. Mag.*, vol. 7, no. 2, pp. 18–21, 2018.