Security and Privacy Aware Communication in Body Area Networks Using Blockchain Technology

Baraa I. Farhan
College of Computer Science & Information Technology, University of Wasit, Wasit, Iraq.
E-mail: bfarhan@uowasit.edu.iq

Rawaa I. Farhan
College of Dentistry, University of Wasit, Wasit, Iraq.
E-mail: ralrikabi@uowasit.edu.iq

Ghaith A. Hussein
College of Computer Science & Information Technology, University of Wasit, Wasit, Iraq.
E-mail: galawady@uowasit.edu.iq

Received March 16, 2021; Accepted June 30, 2021
ISSN: 1735-188X
DOI: 10.14704/WEB/V18SI04/WEB18147

Abstract

With the adoption of assorted gadgets and technology loaded devices, there is need to work on security and privacy while using such platforms. Now, the focus of concern has turned to the overwhelming secrecy, the high performance security, and integrity of the transactions in the cyber space. In relation to a chain of records which is interlinked and highly encrypted due to the involving hashing and encryption each process, it is known as a blockchain. The blockchain removes the possibility of a fraudulent or accidental tampering with the framework. Blockchain has the ability to store sensor data, as well as the capacity to thwart data falsification. IoT deployment plans are usually complex, and the distributed ledger is particularly well-suited for Internet of Things (IoT) discovery, authentication, and recording of information. Wireless body networks are set to be published here on the use trends of Blockchain deployment using advanced scripting and embedded technology the included incorporation of effectual effects gives the final results as well as opposed to the conventional cryptography approach to security.

Keywords

Body Area Networks, BAN, BAN with Blockchain, Secured WBAN with Blockchain, Secured IoT, Wireless Body Area Network.

Introduction

Several countries are currently employing innovative blockchain based security technologies for a wide variety of use cases including e-government, e-commerce, agriculture, and healthcare, as well as aeronautical and telemedicine. They are looking to integrate blockchain technologies into their projects, and to ensure transaction secrecy as well as the decentralisation.

These are the main drivers of increased visibility and integration in secure blockchains (Gupta *et al*, 2017; Abadi *et al*, 2018) When added to the other features, such as portability. It includes time reduction, irreversible transfers, transparency, and teamwork when added to the other features. Fig. 1 presented how blockchain work.

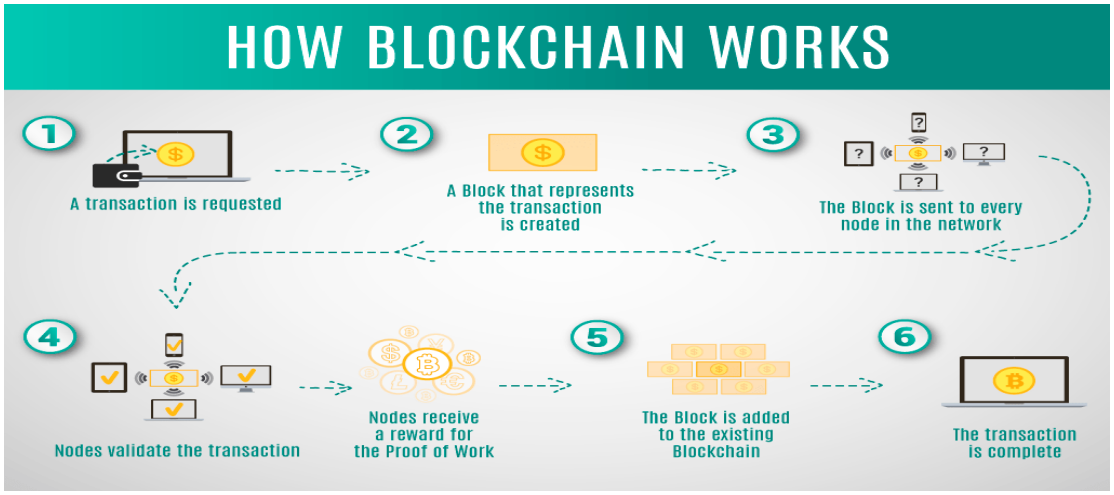

Fig. 1 Blockchain Process Flow

In the blockchain based process flow, transaction is authenticated by the use of advanced protocols and cannot be crushed due to clever network blockchain contracts (Yaga *et al*, 2019).

International Scenarios of Adoption of Blockchain

According to data from Statista, foreign investment reached nearly $3 billion in 2019. Various blockchain use cases range from e-government to e-commerce, but that is not the end of the story, it. In 2018, the agriculture market was predicted to be a long-term business winner for blockchain in the region of $40 million to $400 million.

Centered on a totally integrated blockchain, the UAE has built a smart city. Dubai is often referred to as "the Blockchain's first capital" due to its numerous plans for implementing blockchain technology in everything from real estate to tourism. Blockchain applications

can produce up to $3 billion in cost savings in various sectors of the US, Singapore Airlines uses digital wallets and blockchain in a bold and creative way. As well, which is used in the consumer satisfaction and payment strategy, Singaporeans is highly interested in applying blockchain in education, public administration, healthcare, and the food industry. The use of Aver space in the immobilization industry is very prominent. Many, if not all, of the agreements in this case have been kept digital, which is extremely secure.

Methodology

A. Body Area Networks (BAN) as Main Blockchain Based IoT Deployment

BANs is an active and growth field of health-care provision and monitoring. The fitness monitor is especially relevant to the elderly and people with long-term health issues, since they are already likely to have reduced physical activity levels, but for athletes it provides objective data about how well they are doing their job.

BAN hires sensors and actuators that allow for on or administration of treatment or equipment all over the body; Fig. 2 a main unit with several sub-sensors (for patients with pacemakers) are called DAENS. (LA) (ER) The monitoring and actuating devices are distributed all over the body.

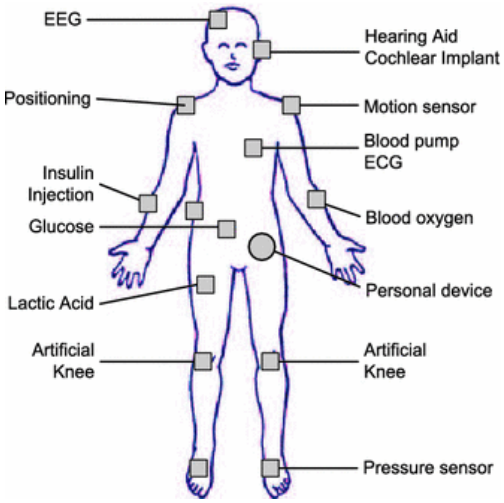

Fig. 2 Key Points for WBAN Integrations

In other words, a body-area network (BAN), referred to as a “wear skin” area network (WBAN) or “clothesline "area” network, or as a clinical-area network (CAN). BAN sensors could be surface-mounted, as inserts, or they might be fixedly placed on the skin, for example, or carried in different bags, such as a backpack. Although the focus on

reducing the number of gadgets is obvious, essential regional sensors will have a tab-and-plus body network (of 10 BSUs) with a body-related work unit (BCU) as in Fig. 3.

Fig 3 FDA Panel Says No to Shock Therapy Device

In around 1995, the WBAN (Wired Personal Area Network) was developed to use communication-on-by-personal-are aspect (COPA) and within/close-proximity (WPAN) devices. More than six years later, "BAN" systems were regarded as BAN systems that only operated on or around the human body. Between age 35 and age 55, if you're unable to run away from a dog, the dog will certainly bite you, but between the ages of 35 and 65, you've already had a lot of nonsense done to you. The WBAN can be used as an entry point for WP (Wireless Broadband Access Network). With wearable devices, the people can connect to the internet through the gateway Regardless of where the patient is located, medical practitioners are able to use the Internet to find records.

A new generation of low energy physiological sensor networks are being employed for traffic management, crop tracking, and health care now that radiological communications have increased. Since it integrates everything inside the clinic, the body network will be able to keep costs down and prevent medical errors by having their records updated in real time. A mix of electronic physiological sensors can be integrated into the wearable body network to help with both medical and rehabilitation measures the composition of these delicate biosens must be fully non-invasive. The sensors implanted in the patient obtain a variety of physiological measurements in order to track the patient's condition. When connected, the data will be sent wirelessly to an external computer.

Clinical telemedicine does not relay any signals in a timely manner, sequential manner; instead, it provides them all at once for every doctor in the world to see in real time. If an emergency may occur, the device automatically notifies the patient by sending necessary alerts. Power able sensors today can provide only a small amount of information and

energy. While it is still in the early days, the area of medical technology, it is expected to produce ground-breaking concepts such as home healthcare and mHealth.

Due to recent advances in integrated circuit technology, computers are being able to detect, supplement, or even substitute the uses of biomedical to as pacemakers. Since they are implanted below the skin, pacemakers take less energy for years on a single battery, these devices are useful for long-term pacemakers and tracheostats that have the option of skin reattachment.

Tiny computer chip which measures body fat stores and sends them instant notifications to you about food and exercise so you can reach your ideal weight, or instant activity reminders so you can reach your ideal activity level the advantage of Network IBANs is that they're intentionally made to differ from other networks in different ways:

It is important to take the power consumption of your computer into consideration. A standard pacemaker has a battery for 7-10 years. Because a patient's battery power needs change many times per day, they should have a rechargeable cell with a light workload that does not need to be recharged often throughout the day

Since implantable devices have to be lightweight, manufacturers must find ways to incorporate components which are larger than reality, engineers face reality-sized components like antennas.

Unlike a standard Wi-Fi networks, which must be located and operated from a location, personal networks such as hotels and Starbucks' would have to travel with the individual and stay in motion. Transmission ranges from the implant to the body worn controller is short. It's difficult to migrate. As the body expends or absorbs the signal that carries the data, it uses the energy of the signal. Sometimes, this phenomenon shifts dramatically.

When we get older, our bodies become less efficient conductors of electricity, which impacts the efficiency of our antennas. You'll find that an antenna that's optimized for a particular frequency works better when it is in contact with the body, for example.

Medical information inside the BAN environments can be monitored this way. an intelligent WBAN which can be used to track medical issues as an alternative, a wireless body area network can be set up. Bio sorption theory claims that tiny sensors in the human body make it possible for biosensors to function. To track the patient's condition, Fig. 4 show different physiological readings are acquired (Bethencourt *et al,* 2007).

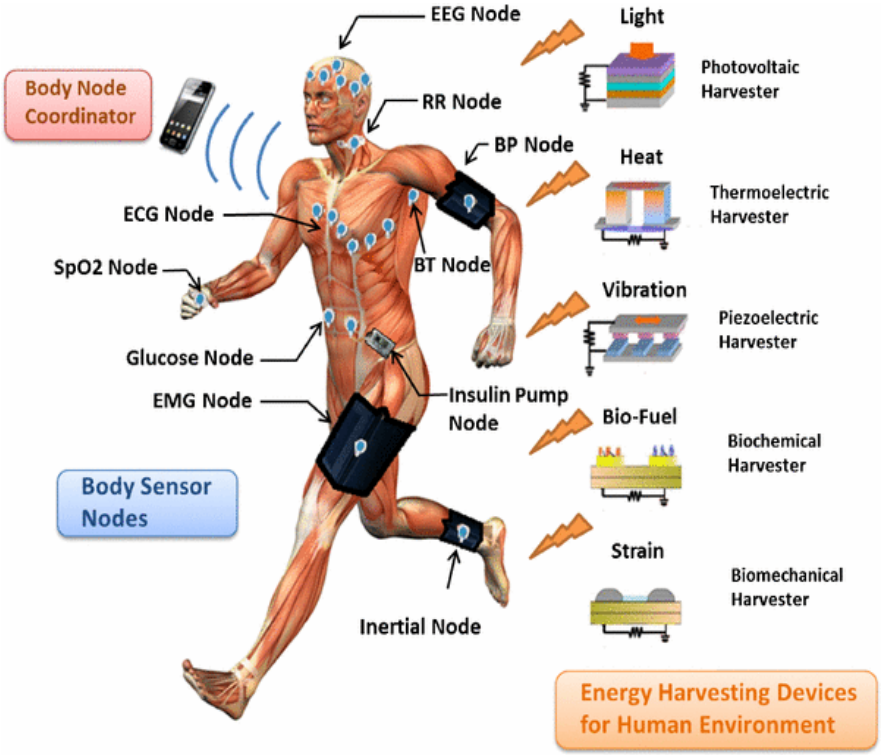

Fig. 4 Logging to BAN of Multiple Body points

B. Medical Applications of BAN

In the healthcare, the initial goals of the BBAN system are mostly chronic conditions such as diabetes, asthma, and heart attacks, which can monitor those.

A patient's BAN can not only inject insulin through a pump when their vital signs are read, but also alert the hospital of those transitions.

The media can be applied to a variety of purposes, including sports, military, or to defence. an expansion of the application to new places may also help people communicate with each other, perhaps with a computer or by way of organic links

C. Applications of Blockchains and BAN other than Telemedicine

Sports -Navigation, timekeeping, distance, pulse rate and body temperature can be calculated by means of sensors.

Military - Can be used to communicate with and send information to a military base commander about threats, withdrawals or running. Lifestyle and entertainment – Web-based music and video calls.

D. Technologies and Frameworks of Blockchain Deployment

A variety of programming systems and technologies are in use for operating with the blockchain Platform implementation is contingent on both on network type, programming language, consensus protocol, and prominence. Building a blockchain system which is reliable and performance needs to be evaluated by one of Blockchain Programming Technologies as in Table 1.

Table 1 High Performance Technologies for Blockchain Programming

URL	Technology / Platform
https://www.hyperledger.org/	Hyperledger
http://iotatoken.com/	IOTA
https://www.corda.net/	Corda
https://github.com/HydraChain/hydrachain	HydraChain
https://www.openchain.org/	OpenChain
https://console.ng.bluemix.net	IBM Bluemix Blockchain
https://erisindustries.com/	Eris
https://www.bigchaindb.com/	BigChainDB
https://chain.com/	Chain
http://www.multichain.com/	MultiChain
https://www.ethereum.org/	Ethereum

Blockchains, and intelligent contracts are the critical features of prominent blockchain and DLT platforms.

Structure programming is important and multi-functional in the guise of Eris is exceptionally able to construct and change well-reasoned, well-structured and swiftly contracts. Reliability and trust can be configured with different applications in private blockchains. Developers use the network to improve intelligent contracts. When smart contracts are in safe environments are introduced, they can verify transactions using innovative agreements.

Often referred to as distributed hydropower, distributed hydropower, approved hydropower, distributed hydropower, and authorized hydropower, these are three different words relating to how electricity is used in hydropower networks. In simple terms, the unique selling proposition of Hydra Chain is their seamless protocol, which works with any Ethereum network. The most important feature of Hydra Chain is to link individuals and businesses to enable peer-to-peer value transfer. Furthermore, configurations native to the Hydra Chain are quicker to build and allow greater versatility and customizability (ideal ready-made contracts do not have the same configuration options)

The words 'open chain' and 'free chain' apply to an open source network. For quick and intense applications in companies and company implementations, it's an excellent resource. As opposed to other networks, the turnaround time is quite a bit faster. A better and standardized peer-to-peer topology with client-server infrastructure is provided by Open Chain. Multiple signing and verification keys are available [Many different keys are given here]. Many Open chain key signatures are available

Open Chain's most critical features are:

- Security of digital signatures
- No mining costs
- Various degrees of control
- Key Privacy
- Transactions checked instantly
- Procedures summary
- Openness and validation management

Ethereum is an open-source platform for developing new blockchain applications. Decentralized applications of Ethereum can be built on all sorts of platforms. The open source community is generally having more security and flexibility across various platforms. Blockchain-based smart contracts can be setup and used on Ethereum. Ethereum supports three programming languages: Go, Python, and C++.

With the foundation now open source, we have launched the cutting-edge blockchain system. A private blockchain can be used for business applications, and networks, as well as decentralized networks. Hyper ledger is programmed in Python. Hyper ledger adds a range of blockchain ventures to its line of product development ledger's. All three of these are part of BESU, SAWS, IRO, and Linen. The blockchain can be audited using AVAL, CALIP, CELL, and EXPLORE.

Since the Internet of Things makes use of sensors or chips, we want to watch the device. Classic RFID-based IoT deployments. The subjects included in the Internet of Things include such diverse instruments as implanted or on-site heart systems, coastal sensors, unmanned marine vessels, fire alarms in motor vehicles, transponders for clams, motor vehicles with built-in or on-site sensors, and targeted biomass. Example smart washers and dryers are available, for example (Zhang *et al*, 2009).

Real-world software is written in a wide variety of languages, including Python, JavaScript, and so on. Programming for the encryption of blocks on Blockchain includes crypto graphing functions. Additionally, cryptography is necessary to ensure that the protection of communication and data processing are needed in smart contract creation.

E. WBAN Using Blockchain

The use of WBAN (Wireless Blockchain Application Network) and blockchains are compatible and are both easy to use because of their independent and joint nature as shown in Fig. 5.

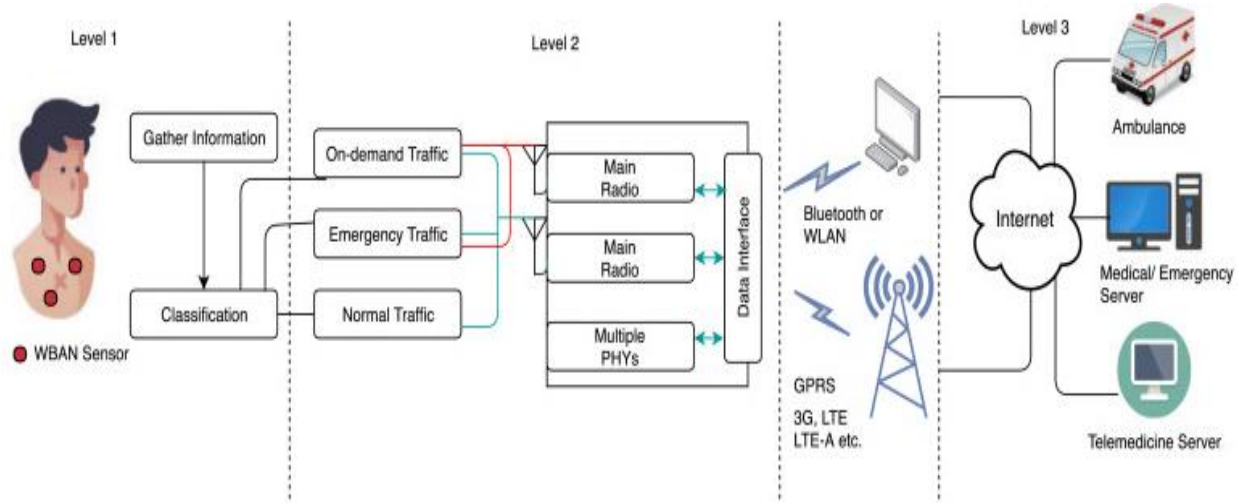

Fig. 5 WBAN Architecture using Blockchain

The block of genesis refers to the first block in the blockchain network. It is the initial block in the blockchain. There's no prior hah value in this block. After this block of genesis, every other block is created and inserted using protocols and intelligent contracts after validation. When the blocks are enabled in the blockchain, the blocks are validated for additional transactions and data transfer.

The fact that the human body's vital signals have been tracked to diagnose diseases early has led to the development of e-health wireless body networks (WBAN). One of the key issues with this technology is to safeguard users' data on the internet and to ensure that it is protected and unavailable for unauthorized individuals or exploited by someone who respects the patient's privacy. In this paper, the Blockchain technology was proposed to secure patient data to protect consumer data and confidentiality, and encryption algorithms have been used to secure the channel of data transfer between the patient and e-health providers (Halperin *et al*, 2008).

The growing number of people with chronic disease has made many suffer from a health condition due to the inability to handle the number of care-related individuals in current traditional medical practices. However, the advent of bio-medical sensors (Lorincz *et al,* 2004) and modern communication techniques like IoT have revolutionized the health care system, especially e-healthcare. E-Healthcare, a non-invasive technology, is essential in remote surveillance of the physical state of the body and assists in conventional medical applications. The proposed framework is based on WBAN networks for networking of patient devices and blockchain technology for data transfer and storage.

Discussion and Results

This study proposes a blockchain-base E-Healthcare system for the provision of a safe and power-efficient medical care solution. The assessment of the approach presented showed that less hardware is required to achieve a high level of safety and reliable performance.

The following Table 2 depicts the security parameter analyzed on simulation with assorted approaches including classical crypto-signal and blockchain based dynamic security with effective security. The traditional approach of crypto-signals includes the key exchange with classical hash generation but it is vulnerable and not effectual for real time scenarios. The implementation patterns of blockchain based security is making use of real time key generation and having its record in the dynamic ledger that is based on the core technologies of blockchain which presented in Table 2.

Table 2 Evaluation Patterns with BAN and Blockchain

Crypto-Signal Based Approach	Blockchain Based Security in BAN
80	88
87	96
80	94
87	92
87	96
83	96
87	96
80	89
86	92
86	89
86	93
84	97
83	96
82	92

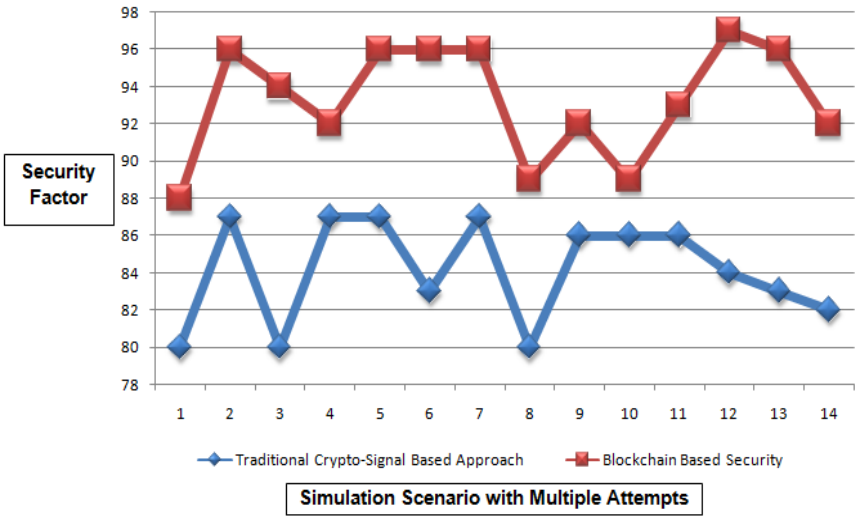

Fig. 6 Evaluation of Performance

The Fig. 6 represents the security elevation in the projected blockchain based approach and quite effective with different attempts of simulation patterns to have the analytics.

A. Blockchain Based BAN for Telemedicine

For example, when the insulin level in the patient's body falls, a WAVE is emitted from the pump and initiates routine administration. It is an excellent multipurpose software Everywhere on the planet, including health care organizations, insurance providers, and manufacturers of medical technology, as well as companies, have been scrutinised for the application of wireless networks. WMANs have risen to prominence in the field of study and have found many varied uses. They want to be a comprehensive supplier of programming for the Internet of Things in the future (IoT+) We realize WBAN has some obstacles to overcome when it comes to the above issues, namely: Network energy usage, interoperability, equipment, sensor authentication, data processing, and system validation. The WBAN standard was finished in 2012 in the world, according to the IEEE task force for WBAN It was founded in 1998 to specialize in WLANs. The assignment was to use a standard component to conduct short-link wireless communications (WFN). As technology is introduced, it becomes an overwhelming success in healthcare.

Despite being wonderful, it has some hidden hazards associated with it. What WBAN does is, is to collect and process various personal details, such as your health, signs of life, etc. It then presents these with prompts to you for your thoughts and asks you if you have any issues. Unauthorized hackers hijackers infiltrate the WBAN to steal user data For example, when a hacker sells data to an insurance provider, such attacks go absolutely compromise the user's privacy. Since the intruder takes control of the WBAN to extract

fake data from the data collector, he tries to. Furthermore, this will alter the user's data, as when the user is a patient, and incorrect data is provided to them, resulting in doctor failure. This paper applies blockchain technology to solve the above challenges by using digital signatures.

Conclusion

Finally, and perhaps most importantly, bear in mind that opinions are based on theories and they are rarely facts. It's even more difficult to use blockchains for electronic government, where data security and data privacy are major issues. In numerous countries around the world, including Singapore, the UAE, Japan, Switzerland, and China, blockchain is being used for a number of different projects. You can use the high-performance and high-security blockchain to store citizens' biometric data, data related to government services, such as physical and educational records, as well as in developing countries like India. Blockchain integration with WBANs (woven biometric applications for the internet of things and/wearable devices) is strong.

References

Abadi, J., & Brunnermeier, M. (2018). *Blockchain economics (No. w25407).* National Bureau of Economic Research.

Bethencourt, J., Sahai, A., & Waters, B. (2007). Ciphertext-policy attribute-based encryption. *In 2007 IEEE symposium on security and privacy (SP'07)*, 321-334.

Carroll, R., Cnossen, R., Schnell, M., & Simons, D. (2007). Continua: An interoperable personal healthcare ecosystem. *IEEE Pervasive Computing*, *6*(4), 90-94.

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation*, *2*(6-10), 71.

Chessa, S., & Maestrini, P. (2003). Dependable and Secure Data Storage and Retrieval in Mobile, Wireless Networks. *In DSN* 2003, 207-216.

Di Pietro, R., Mancini, L.V., Soriente, C., Spognardi, A., & Tsudik, G. (2008). Catch me (if you can): Data survival in unattended sensor networks. *In Sixth Annual IEEE International Conference on Pervasive Computing and Communications (PerCom),* 185-194.

Gupta, S.S. (2017). *Blockchain.* John Wiley & Sons, Inc.

Halperin, D., Heydt-Benjamin, T.S., Fu, K., Kohno, T., & Maisel, W.H. (2008). Security and privacy for implantable medical devices. *IEEE pervasive computing*, *7*(1), 30-39.

Ramachandran, A., Zhou, Z., & Huang, D. (2007). Computing cryptographic algorithms in portable and embedded devices. *In IEEE International Conference on Portable Information Devices*, 1-7.

Kotamraju, S.K., Arepalli, P.G., Vejendla, L.N., & Kanumalli, S.S. (2021). Implementation patterns of secured internet of things environment using advanced blockchain technologies. *Materials Today: Proceedings.*

Jovanov, E., Milenkovic, A., Otto, C., & De Groen, P.C. (2005). A wireless body area network of intelligent motion sensors for computer assisted physical rehabilitation. *Journal of Neuro Engineering and rehabilitation, 2*(1), 1-10.

Venkatasubramanian, K., & Gupta, S.K. (2007). Security solutions for pervasive healthcare. *In Security in Distributed, Grid, Mobile, and Pervasive Computing,* 349-366.

Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering, 59*(3), 183-187.

Morchon, O.G., & Baldus, H. (2008). Efficient distributed security for wireless medical sensor networks. *In International Conference on Intelligent Sensors, Sensor Networks and Information Processing,* 249-254.

Wang, Q., Ren, K., Yu, S., & Lou, W. (2011). Dependable and secure sensor data storage with dynamic integrity assurance. *ACM Transactions on Sensor Networks (TOSN), 8*(1), 1-24.

Zhang, R., Zhang, Y., & Ren, K. (2011). Distributed privacy-preserving access control in sensor networks. *IEEE Transactions on Parallel and Distributed Systems, 23*(8), 1427-1438.

Risius, M., & Spohrer, K. (2017). A blockchain research framework. *Business & Information Systems Engineering, 59*(6), 385-409.

Yu, S., Ren, K., Lou, W., & Li, J. (2009). Defending against key abuse attacks in KP-ABE enabled broadcast systems. *In International Conference on Security and Privacy in Communication Systems,* 311-329.

Yu, S., Ren, K., & Lou, W. (2010). FDAC: Toward fine-grained distributed data access control in wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems, 22*(4), 673-686.

Nishide, T., Yoneyama, K., & Ohta, K. (2008). Attribute-based encryption with partially hidden encryptor-specified access structures. In International conference on applied cryptography and network security, 111-129.

Nosowsky, R., & Giordano, T. J. (2006). The Health Insurance Portability and Accountability Act of 1996 (HIPAA) privacy rule: implications for clinical research. *Annual Review of Medicine, 57*, 575-590.

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. *arXiv preprint arXiv:1906.11078.*

Cheshmeh Sohrabi, M., & Dashtaki, N.A. (2019). Ask search engine: Features and performance identification. *Webology, 16*(1), 77-85.