Medicon Engineering Themes
Volume 1 Issue 1 September 2021
Editorial

Internet of Things, Cryptography, Blockchain and Data security: New Trends and Challenges

Muzafer Saračević*

Department of Computer Sciences, University of Novi Pazar, Serbia

***Corresponding Author:** Muzafer Saračević, Department of Computer Sciences, University of Novi Pazar, Serbia.

Received: August 26, 2021; **Published:** September 01, 2021

Security is a very important aspect of a smart system as one of the core smart city components. That is why the concept of smart cities must pay special attention to the security of the individual Internet of Things (IoT) components that make up smart cities. For an IoT system to operate smoothly, all participants in the communication must permit the system to collect information about them - e.g., on the street by various sensors, at home by various devices, such as mobile devices, etc. Such a large set of data collected about the citizens in a smart city is a major security issue [1].

Also, IoT brings a new set of security concerns, especially when it comes down to data confidentiality, reliability, and integrity. Cryptography is a science that evolves rapidly, and new encryption and data hiding methods and protocols are reported in the relevant literature almost daily. The communication protocols that smart devices employ are simple, but their complexity is conditioned by the hardware limitations and software capabilities of the IoT devices themselves. When developing an IoT platform, it is necessary to consider all the required functional elements, and one of the most important elements of any IoT system is the security component. This segment refers to the authentication and authorization as well as to the protection of privacy and integrity of the data. IoT is highly applicable to various areas, such as transport, traffic, education, and health care. Reliability and security are big problems in all areas, especially in health care. Without security, the integrated development of IoT is virtually impossible in health care institutions. The information should be accessible when necessary, but also confidential. It is the information owner who will decide whom to provide access to the information [2].

Key management is extremely important for the security of the entire communication system. In cryptology-based infrastructure, the majority of attacks are aimed at the key management level. Participants in cryptographic systems must be able to generate keys. If the key is lost or compromised in any other way by any participant in the communication, others must be warned promptly. Otherwise, the adversary will be able to decrypt messages with the stolen key. Since the keys have a limited life expectancy, the most important reason for their periodic replacement is protection against cryptanalysis. The problem of secret key distribution is constantly present since the very beginnings of cryptography [3].

The biggest problem in today's multimedia communications is data security. Because the web environment is organized as a collection of many different participants that use the same protocol to exchange data, it is very difficult to enable absolute control. On the other hand, steganography is a hiding technique that no one but the transmitter and receiver is aware of the existence of communication. The main advantage of steganography to cryptography is the fact that hidden messages do not attract attention to themselves [4].

Insecure transmission of digital data over another network is always open to theft by the administrator of that network. Blockchain technology has several features that are inherently related to security and trust issues. Blockchain is an attractive solution if there is an intention or need for the database to be decentralized. In general, blockchain technology is based on a database that is not in one place but consists of smaller databases (blocks) that are digitally interconnected. One way to convince rights holders of secure transmission is to encrypt material when transiting through the network, and directly decrypt it before the content is broadcast. Once some of the information is added to the end of the chain, it is practically impossible to go back and change the content of that block, because each new block is inextricably linked to the one after it [5]. In other words, once a block is added, it is very difficult to change, and it is impossible to delete it. When it comes to trust, blockchain networks implement tests for computers that want to join the chain and add blocks. This concept of encrypting multimedia materials serves not only to prevent access by persons who do not have the right to do so but also to prevent the illegal production of digital copies.

References

1. Saračević M., et al. "Cryptographic Keys Exchange Model for Smart City Applications". IET Intelligent Transport Systems 14.11 (2020): 1456-1464.
2. Saračević M., et al. "Data Encryption for IoT Applications Based on Catalan Objects and Two Combinatorial Structures". IEEE Transactions on Reliability 70.2 (2021): 819-830.
3. Saračević M., et al. "Source and Channel Models for Secret-key Agreement Based on Catalan Numbers and the Lattice Path Combinatorial Approach". Journal of Information Science and Engineering 37.2 (2021): 469-482.
4. Saračević M., et al. "A novel approach to steganography based on the properties of Catalan numbers and Dyck words". Future Generation Computer Systems 100 (2019): 186-197.
5. Saracevic M., et al. A Novel Block Encryption Method based on Catalan Random Walks, Multimedia Tools and Applications, Springer Nature (2021).

Volume 1 Issue 1 September 2021
© All rights are reserved by Muzafer Saračević.