Aao Huzoor Tumko By Jonita | Email - Pabak Indu - Outlook | IQAF-Criteria 3.xlsx | (1) WhatsApp | InSc - AWARDS | Early Work Vis-à-Vis Current Tren
link.springer.com/chapter/10.1007%2F978-3-030-50244-7_8
Apps | Database System C... | The C++ Standard... | WhatsApp | Reading li

Innovations in Cybersecurity Education pp 127-156 | Cite as

Early Work Vis-à-Vis Current Trends in Internet of Things Security

Authors | Authors and affiliations

Pabak Indu, Souvik Bhattacharyya

Chapter
First Online: 22 November 2020

175
Downloads

Abstract

IoT has contributed heavily in the growth of Internet with its versatile applications. The IoT devices act as a bridge between the digital world and the real world. Therefore, the previous embankment of securities does not keep all these attacks at bay in recent years. Still, it is undeniable that IoT devices have become an integral part of our daily life. From emergency notification systems to health monitoring devices, IoT plays a vital role. As the versatility of the IoT devices is expanding, so the security challenges. The security issues impacting the IoT devices have become an enormous concern for the organizations spread across the world. The root cause of modern security threats in IoT devices is the lack of refined cybersecurity implementation towards real-time communications, data sharing, remote access, etc. For every smart business or home solutions, it is essential to provide suitable cybersecurity solutions in IoT devices to maintain their supremacy in the future digital world. The IoT devices most often become vulnerable towards modern security threats because of their elementary level security protocol.

To understand the vulnerabilities of IoT, we need to identify the attack vectors and provide the corresponding remediation methodologies proposed by the present-day researchers. Along with the remedial methodologies, several real-time security issues have been identified, responsible

Chapter EUR 24.95
Price excludes VAT (India)

- DOI: 10.1007/978-3-030-50244-7_8
- Instant PDF download
- Readable on all devices
- Own it forever
- Exclusive offer for individuals only
- Tax calculation will be finalised during checkout

Buy Chapter

eBook EUR 96.29
Hardcover Book EUR 119.99

Learn about institutional subscriptions

Cite chapter

Advertisement

springer.com
Make your move to publishing open access today.
We're widely read with an impact in the field.

Springer
Hide

Type here to search
27°C Haze ENG 09:44 AM 04-11-2021

Aao Huzoor Tumko By Jonit | Email - Pabak Indu - Outlook | IQAF-Criteria 3.xlsx | (1) WhatsApp | InSc - AWARDS | Real-Time Watermarking of Mec | Hiding IoT Communication Usin
link.springer.com/chapter/10.1007/978-981-33-6915-3_49
Apps | Database System C... | The C++ Standard... | WhatsApp | Reading
Springer Link
Search | Home • Log in

Advances in Medical Physics and Healthcare Engineering pp 497-506 | Cite as

Real-Time Watermarking of Medical Images and Secure Transmission Through Steganography

Authors | Authors and affiliations

Ajay Biswas, Pabak Indu, Souvik Bhattacharyya

Conference paper
First Online: 17 June 2021

170
Downloads

Part of the Lecture Notes in Bioengineering book series (LNBE)

Abstract

Medical images and reports are highly confidential information and should not be leaked, or modified in any circumstances. Healthcare organizations constantly face cyber-attacks with the motive of stealing medical information for their personal gains, and during the COVID-19 pandemic, the attacks have almost doubled. Encrypting medical information and transmitting them over a secure channel ensures the confidentiality of information, however, can be stolen and decrypted later. Also, most of the health organization lacks in terms of security and privacy of their patient's information. A real-time watermarking and steganography protocol can mitigate the aftermath of a cyber-attack by hiding confidential reports into useless looking files such as log files and user manuals as soon the reports are generated. We propose a secure steganographic medical report system that can hide medical reports as well as identify fake ones. The system uses real-time watermarking during report generation which prevents any kind of modification; thereafter, these data are transmitted/stored using a secure steganography protocol. Finally, the data is retrieved by doctors or health workers after stego-extraction and watermark verification

Chapter EUR 24.95
Price excludes VAT (India)
- DOI: 10.1007/978-981-33-6915-3_49
- Instant PDF download
- Readable on all devices
- Own it forever
- Exclusive offer for individuals only
- Tax calculation will be finalised during checkout

Buy Chapter

eBook EUR 160.49
Hardcover Book EUR 199.99

Learn about institutional subscriptions

Cite paper

Type here to search
27°C Haze ENG 09:43 AM 04-11-2021