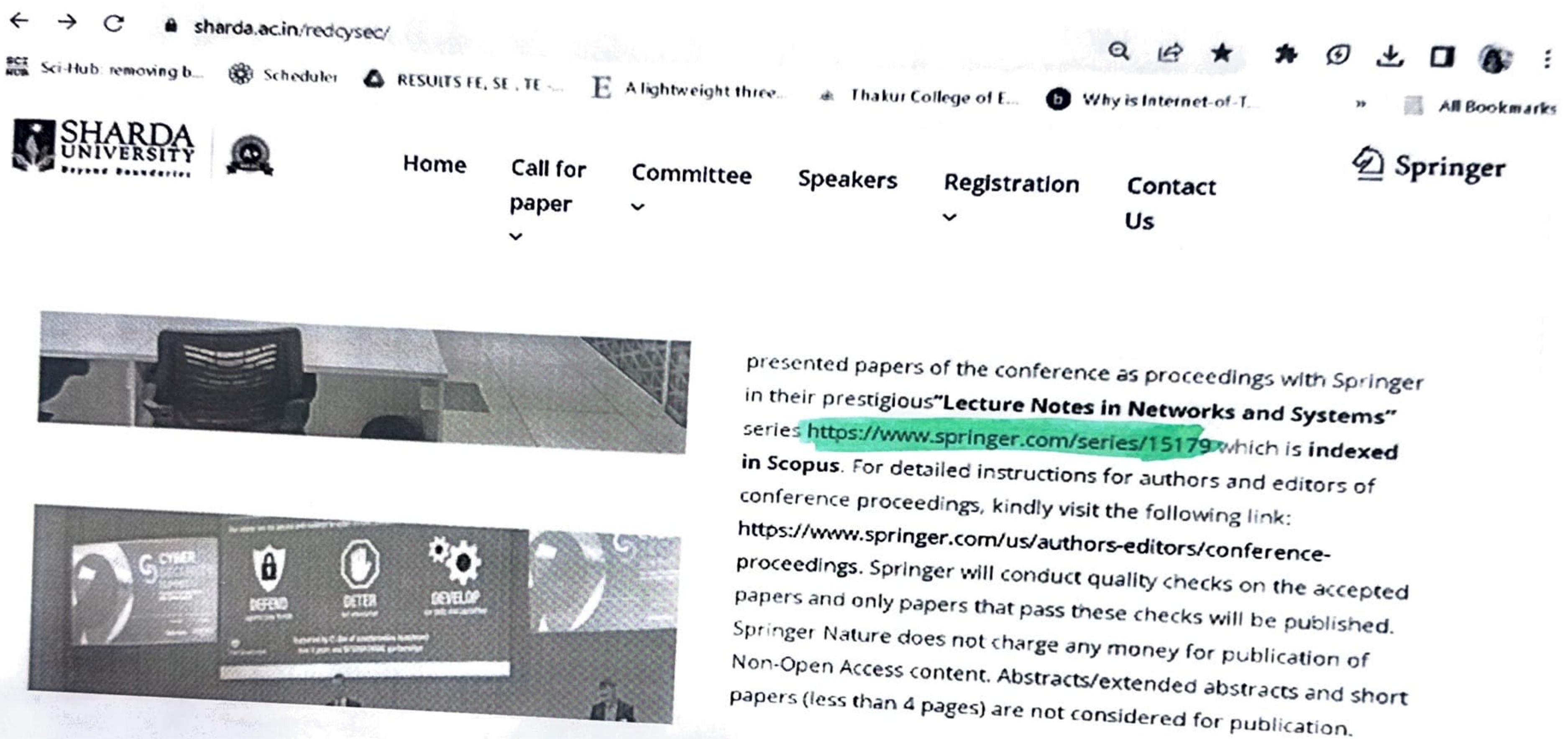
16_Hybrid Lightweight Cryptography using AES and ECC for IoT Security

3.3.2

22-23

18

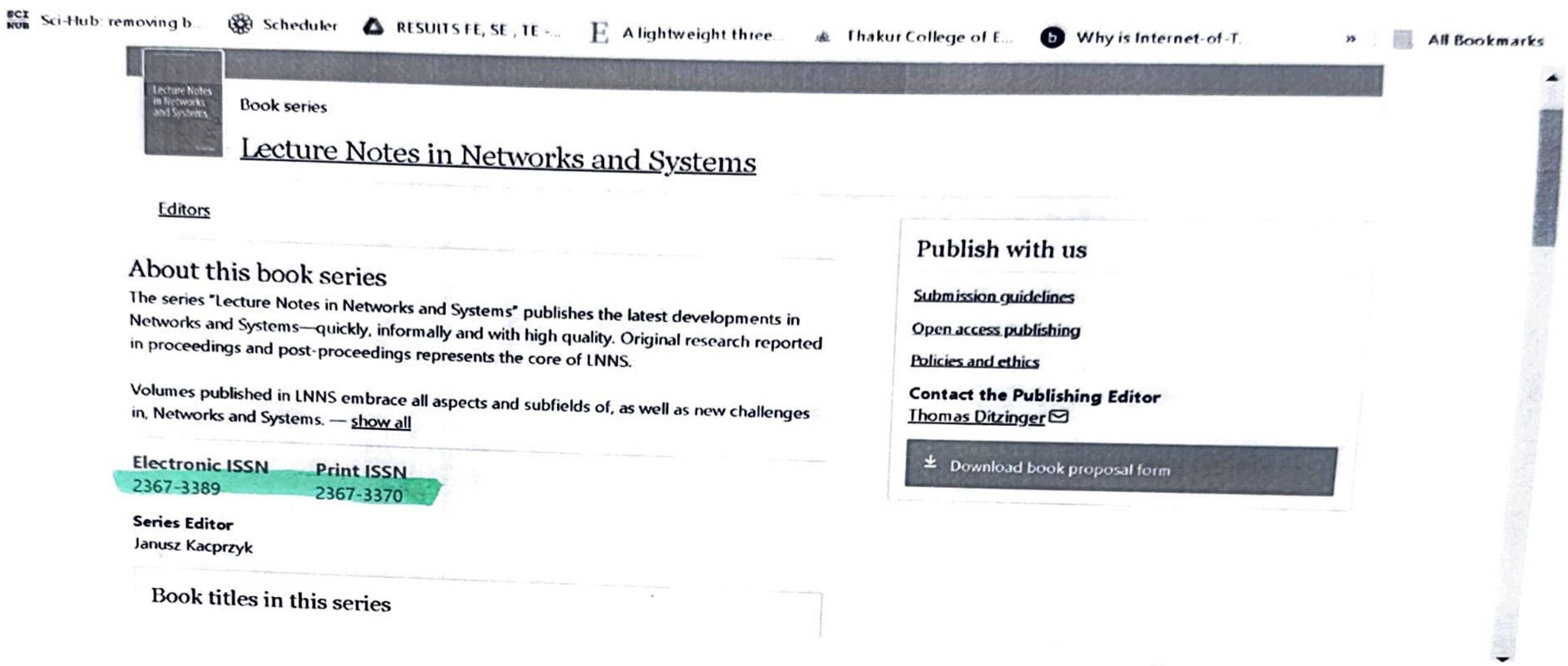


sharda.ac.in/redcysec/

presented papers of the conference as proceedings with Springer in their prestigious**"Lecture Notes in Networks and Systems"** series https://www.springer.com/series/15179 which is **indexed in Scopus**. For detailed instructions for authors and editors of conference proceedings, kindly visit the following link: **https://www.springer.com/us/authors-editors/conference-proceedings**. Springer will conduct quality checks on the accepted papers and only papers that pass these checks will be published. Springer Nature does not charge any money for publication of Non-Open Access content. Abstracts/extended abstracts and short papers (less than 4 pages) are not considered for publication.

VIDYAVARDHINI'S COLLEGE OF ENGINEERING & TECHNOLOGY
EXTC
Engg.

HEAD
Dept of Electronics and
Telecommunication Engg.,
Vidyavardhini's College of
Engineering & Technology
Vasai Road 401 202



Book series

Lecture Notes in Networks and Systems

Editors

About this book series

The series "Lecture Notes in Networks and Systems" publishes the latest developments in Networks and Systems—quickly, informally and with high quality. Original research reported in proceedings and post-proceedings represents the core of LNNS.

Volumes published in LNNS embrace all aspects and subfields of, as well as new challenges in, Networks and Systems. — show all

Electronic ISSN 2367-3389

Print ISSN 2367-3370

Series Editor
Janusz Kacprzyk

Book titles in this series

Publish with us

Submission guidelines

Open access publishing

Policies and ethics

Contact the Publishing Editor
Thomas Ditzinger ✉

Download book proposal form

VIDYAVARDHINI'S COLLEGE OF ENGINEERING & TECHNOLOGY
EXTC
Engg.

HEAD
Dept of Electronics and
Telecommunication Engg.,
Vidyavardhini's College of
Engineering & Technology
Vasai Road 401 202.

Hybrid Lightweight Cryptography using AES and ECC for IoT Security

Mrs. Neha N. Gharat
Thakur College of Engi. &Tech.
Nehagharat10@gmail.com

Dr. Lochan Jolly
Thakur College of Engi. &Tech.
lochan.jolly@thakureducation.org

Abstract: The Internet of Things (IoT) transforms everyone's life by providing features such as controlling and monitoring connected smart objects. The Internet of Things (IoT) architecture is intricate and sophisticated, owing to the substantial number of interconnected devices, diverse link-layer technologies, and multiple services integrated within the system. The adaptation of these devices is increasing exponentially, which creates an extensive amount of data for processing and analyzing. Designing security solutions for the Internet of Things (IoT) requires acknowledging the novel security and privacy challenges that emerge due to the nature of this technology. Securing end-to-end connections in IoT poses a significant challenge due to the heterogeneous nature of IoT communications, as well as the disparities in resource capabilities across IoT devices. Due to the limited computing power, energy, and memory of most IoT devices, the number of security solutions available is limited. Many established security mechanisms cannot be supported by low-capacity devices, narrowing down the potential choices for IoT security solutions. As a result, IoT requires robust security solutions that can efficiently meet specific security and privacy requirements while having a lightweight impact on device resources such as microcontrollers, memory, and energy. The feature of the work is the design of a Hybrid Lightweight Cryptography to enable secure data in IoT against IoT attacks. One of the security fundamentals to secure IoT data is to design lightweight cryptography for IoT devices that are resource-constrained in terms of computational capability, memory space, and battery power. To find an effectual and lightweight key establishment the combination of symmetric and asymmetric encryption algorithms i.e. Hybrid lightweight cryptography is proposed. The primary functionality of the proposed system revolves around the integration of ECC and the Advanced Encryption Standard (AES) method. This combination is employed to uphold data integrity. Security analysis is conducted to prove the scheme fulfills the security requirements and evaluated the performance in terms of computational cost, computational cost, power consumption, memory, and key size.

Keywords: Lightweight cryptography, AES, ECC, Hybrid Cryptography.

1. **Introduction:** The Internet of Things is about the change in the modern control and monitoring of connected smart objects by their features. The IoT is an evolving technology worldwide, which facilitates the connection of sensors, home appliances, automobiles, and offices. IoT architecture provides various smart applications. IoT architecture is multifaceted as various devices, technologies, and services are integrated into the system. The increasing use of these devices creates a very high amount of data