Findings

Notification No.: 593/2026
Date of Award: 02/02/2026

Name of the Scholar: Kamakshi Gupta
Name of the Supervisor: Prof. Syed Afzal Murtaza Rizvi
Name of the Department: Department of Computer Science
Topic of the Research: **"Study on Light Weight Cryptographic Protocols for Secure Communication in IoT"**

The thesis entitled "**Study on Light Weight Cryptographic Protocols for Secure Communication in IoT"** presents the rapid proliferation of Internet of Things (IoT) devices across various domains from smart homes and healthcare to industrial control systems has brought with it a pressing need for robust and efficient security solutions. This research has taken a significant step toward addressing these limitations by proposing two novel lightweight protocols: **LSAP (Lightweight Secure Authentication Protocol)** and **LKDP (Lightweight Key Distribution Protocol)**.
The **LSAP protocol** ensures secure and mutual authentication between devices and the trusted authority (TA) using minimal computational overhead. It provides a defence mechanism against various common cyber threats such as replay, impersonation, and man-in-the-middle attacks, without the need for expensive cryptographic operations.

Similarly, the **LKDP protocol** facilitates a secure and scalable key distribution process. By utilizing lightweight symmetric encryption and hash-based mechanisms, it enables efficient session key generation, distribution, and secure communication among devices in a resource-constrained network.

The modular structure of both protocols makes them adaptable and extensible, allowing for integration into diverse IoT architectures. The emphasis on using HMACs, nonces, and secure key derivation functions ensures that security is not compromised, while performance metrics remain optimal. In addition, the proposed key management mechanism effectively handles device identities and keys through a centralized TA, ensuring both simplicity and scalability.

The thesis is structured into six chapters, summarized as follows:

The ***Chapter 1*** is as usual an **Introduction**, cover basic concepts and the background detail required to understand the topics properly. It has briefly explained the topics Cryptography Symmetric Key Cryptography, Asymmetric Key Cryptography, Hash Functions, Hybrid Cryptography and Lightweight Cryptography.

The **Chapter 2** provides an overview of key IoT security concepts. It explains the **role of cryptography in IoT security**, highlighting how encryption, hashing, and authentication mechanisms protect IoT devices and data. The chapter also describes the **IoT architecture and communication models**, outlining how devices, networks, and applications interact in different communication patterns. Finally, it discusses the essential **security requirements in IoT**, such as confidentiality, integrity, authentication, privacy, and availability, which are

necessary for building secure and reliable IoT systems. The last section of this chapter is literature review.

The ***Chapter 3***, focuses on advanced lightweight security mechanisms designed for IoT systems. It describes various **lightweight cryptographic protocols for IoT security** and presents the proposed **Lightweight Key Distribution Protocol (LKDP)** for efficient and secure key management in constrained networks. The chapter also introduces enhancements to the **Lightweight Secure Authentication Protocol (LSAP)** to strengthen device authentication. Additionally, it highlights innovations in lightweight cryptography and key management that improve IoT security, privacy, and scalability. Overall, this chapter addresses key challenges and offers optimized solutions tailored for resource-limited IoT environments.

The ***Chapter 4***, describes the communication mechanisms used in IoT systems and the security measures required to protect them. It explains how IoT devices exchange data across various networks and outlines the threats, vulnerabilities, and protection techniques associated with IoT communication. The chapter focuses on ensuring secure data transmission, reliable connectivity, and robust protection against attacks in IoT environments.

The ***Chapter 5*** presents the **proposed framework for secure communication** in IoT environments. It outlines the architecture, components, and operational flow of the framework, showing how the proposed protocols ensure confidentiality, authentication, integrity, and efficient key management. This chapter demonstrates how the framework enhances overall IoT security while addressing resource constraints.

The ***Chapter 6*** summarizes the key findings, contributions, and outcomes of the research. It highlights the effectiveness of the proposed lightweight protocols and secure communication framework. The chapter also identifies limitations and suggests future research directions, including improvements in protocol efficiency, scalability, and adaptability to emerging IoT technologies.

This work has contributed to the understanding of how lightweight cryptographic protocols can be both **secure and practical** for real-world IoT systems. By analysing cryptographic operations, key management, and performance-security trade-offs, the research offers valuable insights into the design principles of efficient security mechanisms tailored for the IoT ecosystem. This research not only addresses current challenges in IoT security but also opens pathways for future advancements in the field of lightweight and quantum-resistant cryptographic protocols.