Volume 14, Issue 2
April 2025

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

Lightweight Cryptographic Protocols for IoT: Addressing Security, Privacy, and Scalability Challenges

[1]Kamakshi Gupta and [2]Syed Afzal Murtaza Rizvi

[1,2] Department of Computer Science, Jamia Millia Islamia, New Delhi, India

E- mail: [1]Kamakshigupta630@gmail.com,[2]sarizvi@jmi.ac.in

ABSTRACT

The meteoric rise of the Internet of Things (IoT) and other resource-constrained systems has increased the demand for lightweight cryptography. These techniques aim to ensure essential security with minimal overhead, crucial for constrained IoT environments." Ensuring secure communication in IoT networks while minimizing computational overhead remains a major challenge. Similarly, healthcare systems require strong data protection despite limited device capabilities. Industrial control systems, smart grids, and vehicular networks demand real-time security without compromising performance. This paper presents a comprehensive analysis of lightweight cryptography, discussing its significance, advancements, and Constraints. Existing solutions have been evaluated, and future research directions have been explored, providing practical perspectives for researchers and developers working to secure IoT infrastructures.

Keywords: Lightweight Cryptography, IoT Security, Resource-Constrained Devices, Secure Communication, Cryptographic Challenges.

1. INTRODUCTION

The term "Internet of Things" (IoT) refers to the vast network of interconnected devices that engage in Internet-based communication. In this sense, a "thing" is any item that has been given a unique identification, such as an IP address or device ID, whether it be a human, an animal, or a physical or virtual object. After gathering information from their environment, devices send it to a server over the Internet for processing. There are two primary types of IoT devices.

- **Physical objects**: These include devices like smartphones, cameras, sensors, vehicles, drones, etc.
- **Virtual objects**: These are digital entities such as electronic tickets, calendars, books, and wallets.

IoT devices are capable of remote sensing, performing actions (actuating), and supporting monitoring tasks. By facilitating smooth communication between computer systems and the real world, the Internet of Things aims to decrease the need for human involvement while increasing overall performance, accuracy, and cost efficiency.

IoT developers and administrators face the challenge of selecting the right platform that aligns with their needs, [27-30] based on factors like cost, available APIs, programming languages, and supported devices. While developers and administrators are primarily concerned with ensuring their systems function properly, security and privacy concerns in IoT are becoming increasingly prominent.

Lightweight cryptographic algorithms are optimized to provide strong security while minimizing resource consumption. They achieve this by using smaller key sizes, simpler mathematical operations, and more efficient methods that reduce the computational load. By using these lightweight algorithms, devices can ensure data privacy and security without overburdening their limited hardware capabilities. This makes them ideal for environments where maintaining energy efficiency and performance is critical, allowing devices to function securely for longer periods without requiring significant hardware upgrades or frequent recharging.

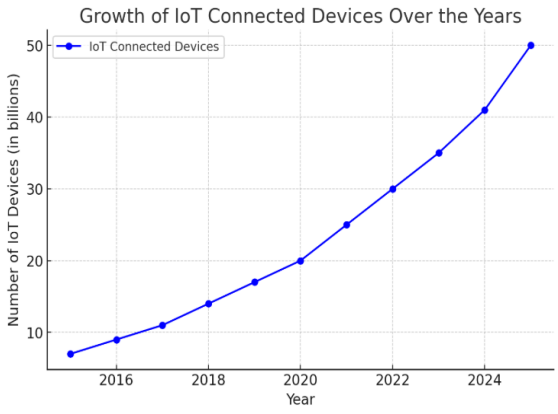

Fig1: Growth of IoT connected devices over the years

Volume 14, Issue 2
April 2025

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

Apart from guaranteeing functionality, IoT users must either possess expertise in security and privacy or have faith in the security measures offered by the IoT platform to uphold a secure environment—a task that is not always simple.Even though a number of IoT security solutions have been put forward, they frequently concentrate on certain designs and fall short of providing all-encompassing defenses that take into account the requirements of different platforms at once.

2. MOTIVATION

The motivation to study lightweight cryptography in IoT networks lies in the need to provide strong security guarantees—such as ensuring data privacy (confidentiality), verifying the authenticity of users and devices (authentication), and maintaining data integrity—while minimizing the computational burden on these resource-limited devices. Lightweight cryptographic solutions offer a way to achieve these security objectives without draining device resources or sacrificing performance.

A survey of IoT applications focusing on lightweight cryptography is essential for understanding how these techniques can be effectively implemented to address the unique security threats of IoT networks. By developing and evaluating cryptographic protocols tailored to the specific constraints of IoT devices, we can enhance the overall security and reliability of IoT systems, making them safer and more efficient for users.

3. ORGANISATION

The paper is organized as follows: **Section 2** highlights the motivation for lightweight cryptographic protocols in IoT, emphasizing the growing security vulnerabilities and threats in IoT communication. **Section 3** provides a structured foundation for the paper. **Section 4** provides a brief review of related work, analysing existing cryptographic techniques and their effectiveness in securing IoT systems. **Section 5** explores various communication protocols in IoT, discussing their impact on security and efficiency. **Section 6** delves into security vulnerabilities addressing authentication attacks and cryptographic limitations in resource-constrained IoT environments. **Section 7** examines privacy concerns, focusing on data protection, user anonymity, and access control mechanisms. **Section 8** identifies key issues and shortcomings in implementing lightweight cryptography, including computational constraints, scalability, and interoperability. **Section 9** presents IoT security solutions, evaluating lightweight encryption techniques, key management strategies, and authentication mechanisms. **Section 10** outlines future research directions in lightweight cryptography, highlighting advancements such as AI-driven security and post-quantum cryptography. Finally, the paper is concluded by summarizing key findings and emphasizing the importance of secure and efficient lightweight cryptographic solutions in IoT communication.

4. RELATED WORK

Clustered Wireless Sensor Networks (CWSNs) are often deployed in unprotected settings, making them susceptible to a range of cyberattacks that impair their functionality. Given the dynamic nature of the network and the resource limitations of sensor devices, creating an effective cryptographic method for CWSNs is extremely difficult. In order to provide mutual authentication while lowering computational and communication overhead, Mezrag et al. [1] offer IBAKAS, an identity-based authentication and key agreement technique that combines Identity-Based Cryptography (IBC) with Elliptic Curve Cryptography (ECC).

Khashan et al. [2] proposed FlexCrypt scheme, incorporating a dynamic clustering technique and an adaptive lightweight cryptographic method to optimize encryption based on available resources. The scheme improved network lifetime by up to 94% compared to existing ciphers and demonstrated resistance to multiple attacks, including brute-force and man-in-the-middle attacks.

Wireless sensor networks, known for their versatility and dense distribution, played a crucial role in various application domains. Among the key technical issues, ensuring security across wireless links remained a critical concern to guarantee data reliability and trustworthiness. Tiberti et al. [3] extended a previously developed cryptographic scheme, termed the topology-authenticated key scheme 2, which leveraged hybrid cryptography to enhance security for resource-constrained sensor nodes.

Ad hoc mobile sensor networks, composed of resource-constrained sensor nodes, emerged as a cost-effective solution for diverse monitoring applications. However, addressing security threats in such networks remained a critical challenge. Delgado-Mohatar et al. [4] presented a lightweight authentication model that leveraged symmetric cryptographic primitives with minimal computational overhead. Comparative analysis with existing protocols, such as SPINS and BROSK, demonstrated significant energy efficiency improvements, achieving reductions of up to 98% and 67%, respectively. Additionally, the proposed model exhibited enhanced scalability by requiring only a single message exchange, regardless of network size.

Mobile ad hoc networks' dynamic and unexpected topology made it difficult to provide dependable group communication. To address these issues, Luo et al. [5] introduced PILOT, a probabilistic lightweight group communication system that leveraged gossip mechanisms and quorum systems. The proposed two-layer system provided reliable multicasting and data sharing while balancing fault tolerance and communication overhead. Performance analysis and ns-2 simulations demonstrated PILOT's predictability and tunability in achieving an optimal trade-off between reliability and efficiency.

Millions of devices interacting inside IoT-enabled LTE/LTE-A networks led to a fast expansion of machine-to-machine (M2M)

communication. A number of key agreement (AKA) and group-based authentication protocols were developed to provide safe machine-type communication device (MTCD) verification. However, these protocols struggled with the single key problem, lacked group key unlinkability, and remained vulnerable to identified attacks. Additionally, some protocols required each MTCD to authenticate independently, causing network congestion. To address these Weaknesses, Parne et al. [6] proposed the Security Enhanced Group-Based (SEGB) AKA protocol, which resolved the single key issue, ensured key forward/backward secrecy, and reduced signalling congestion. Comparing the protocol to other AKA protocols, the formal security analysis showed that it was more resilient to known threats and performed better in terms of network overhead and security needs.

To mitigate authentication signalling congestion and reduce overhead, Lai et al. [7] introduced the GLARM scheme as a lightweight group authentication mechanism to support the authentication of a large number of MTC devices in 3GPP networks. It authenticated all devices within a group simultaneously while minimizing authentication overhead. Security analysis confirmed its robustness, and performance evaluation demonstrated its efficiency, reducing signalling overhead by at least 60% compared to existing schemes, thereby alleviating authentication signalling congestion in 3GPP networks.

Over the past decades, traditional medical privacy data faced significant risks of exposure to third parties or adversaries, particularly from insurance companies, which could compromise individual privacy and disrupt the healthcare industry. RFID-enabled systems gained popularity for privacy protection in healthcare, though they remained vulnerable to tampering and forgery. To address these issues, Shariq et al. [8] proposed a secure RFID-based authentication protocol using a vector space approach to enhance security and privacy. The protocol was evaluated through formal security analysis and demonstrated improved performance in terms of computation, communication cost, and privacy protection compared to existing protocols.

Mutual authentication has become a key mechanism to safeguard RFID systems, ensuring confidentiality, integrity, and authentication. Tewari et al. [9] proposed a lightweight mutual authentication protocol for RFID systems, using minimal computations based on hash and bitwise operations, ensuring mutual authentication, anonymity, and forward secrecy while maintaining low computational costs by avoiding heavy cryptographic algorithms. A comprehensive security and performance analysis confirmed the protocol's effectiveness, demonstrating its advantages over other approaches. Compared to existing methods, this approach was simpler to understand and implement, providing better performance with minimal computational resources.

A blockchain-based secure biomedical image processing system was developed by Rosner et al. [10] to address privacy and security vulnerabilities in cloud-based Healthcare 4.0 systems. The proposed architecture integrated edge, fog, cloud storage, and blockchain layers, utilizing lightweight cryptographic techniques such as ECC, ECDH, and ECDSA. Experimental evaluations with chest X-ray and CT images demonstrated improved computational efficiency, reduced encryption and decryption time, and enhanced PSNR and MSE performance.

IoT services, particularly in e-health applications, raised significant security issues, such as the authentication of connected devices and data exchange. To address these, Almulhim et al. [11] proposed a group-based lightweight authentication scheme that used elliptic curve cryptography (ECC) for enhanced security. This scheme improved energy efficiency, reduced communication distances, and made the network more resistant to attacks.

Increasing use of resource-constrained devices, has enhanced automation, cost efficiency, and real-time data processing. Bayılmış et al. [12] systematically evaluates various communication protocols based on critical factors such as delay, throughput, and energy consumption to optimize QoS in IoT applications. A comprehensive analysis of CoAP, MQTT, and WebSocket was conducted, focusing on their architectural frameworks, security mechanisms, and applicability in diverse scenarios. The findings reveal that CoAP is most suitable for high-traffic, low-energy applications, MQTT excels in secure multi-subscriber communication, and WebSocket facilitates high data rates.

Han et al. [13] proposed a blockchain-based ecosystem to enhance privacy preservation in the Internet of Things (IoT). For asynchronous block validation and leader optimization, a two-sided rating system guaranteed consensus, and a Stackelberg game model with full information feedback was created to promote cooperation. The proposed system effectively balanced resource utilization and security through controlled task distribution. Performance evaluations demonstrated its adaptability to smart IoT environments by enabling controlled and traceable data flow, ultimately improving private blockchain efficiency Future directions include integrating reinforcement learning and swarm intelligence to refine collaboration strategies using distributed AI agents.

The Internet of Things (IoT) comprises an intelligent infrastructure integrating self-organizing devices that monitor the environment and exchange sensitive data with minimal human intervention. However, the vast network of resource-constrained, battery-powered devices faces significant security and privacy pitfalls. Rao et al. [14] analyzed various lightweight security solutions for IoT applications, emphasizing the need for efficient cryptographic mechanisms. Additionally, the review explored the Microsoft Threat Modeling Tool (TMT) as a security assessment framework within the secure development life cycle (SDLC) of IoT applications.

To enhance security and privacy, a lightweight cipher approach was proposed, for validating nodes, users, and devices in 5G networks. A novel dynamic key generation scheme was introduced, by Pothumarti et al. [15] which continuously produced unique keys without relying on constant key negotiation. Performance evaluation demonstrated improved security, reduced communication overhead, and lower latency across various IoT applications in 5G networks.

Hsieh et al. [16] addressed security breaches in vehicular networks, particularly focusing on key agreement and secure communication among high-mobility vehicles. An asymmetric key mechanism and group-based Elliptic Curve Cryptography (ECC) were applied to authenticate data propagation and secure group communication. A flooding delay mechanism was introduced to minimize broadcast collisions, with vehicles individually calculating propagation delays. Two group key agreement schemes were proposed for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) modes, ensuring secure communication. Security analysis demonstrated that the schemes effectively prevented unauthorized vehicle participation, while evaluation results confirmed that the delay mechanism improved data flooding performance with acceptable delay times.

Shao et al. [17] proposed a provably secure lightweight authentication mechanism based on elliptic curve signcryption (EPSLA) for vehicle-to-vehicle (V2V) communication. The EPSLA scheme provided strong security against message forgery, confidentiality breaches, and privacy violations, even in resource-constrained devices. By minimizing scalar multiplication operations and introducing batch unsigncryption, improved computational efficiency and reduced communication costs, outperforming existing mechanisms in both security and performance.

The Internet of Vehicles (IoVs) recently gained attention for enhancing vehicle safety, infotainment, and traffic efficiency. However, authentication and secure communication remained key overheads. To overcome this, a lightweight mutual authentication protocol was designed using cryptographic operations, allowing devices and servers to establish a secret key for secure communication while minimizing computational costs. The protocol was implemented on two communication models—one using a Trusted Authority and another using a Vehicle Server— Vasudev et al. [18] demonstrating improved performance compared to existing systems.

V2V communication became crucial due to the rise in traffic accidents and advancements in information sharing. Ensuring secure and reliable data transfer was essential for maintaining trust among vehicular network users. To address latency and computational complexity issues, blockchain technology was utilized Kamal et al. [19] for real-time data authentication. Link fingerprints were generated using wireless channel characteristics, enabling efficient adversary detection. The approach proposed demonstrated low time complexity, ensuring a lightweight and secure solution for V2V communication in IoV networks.

Vehicular communications had become essential in improving safety and business applications, providing benefits to users through V2V communication for direct exchange of information between nearby vehicles. However, existing message dissemination methods struggled with security threats, high execution times, and communication overhead, hindering real-time communication. To address these issues, a secure and efficient V2V data transmission protocol utilizing a one-way hash function was proposed by Limbasiya et al. [20]. The results demonstrated improved execution times, reduced storage costs, and lower communication overhead, while maintaining resilience against multiple security attacks. The enhanced protocol, employing low-cost cryptographic functions, offered significant improvements in performance, making it suitable for secure and rapid information exchange in smart city applications.

To address the concerns of secure data sharing and model training in intelligent transportation systems. Huang et al. [21] proposed a distributed machine learning framework, DSL, which integrated edge computing, federated learning, and blockchain technologies to ensure reliable data sharing and asynchronous model training in IoVs. To handle vehicle mobility, authors developed a dynamic vehicle association (DVA) algorithm, optimizing connections between vehicles and roadside units to improve training efficiency. By incorporating a DAG-based blockchain, authors enhanced the security of the DSL algorithm with an attack detection method and an accuracy-based reward mechanism. Simulation results demonstrated the superior performance of the proposed DSL algorithm

To improve security in smart city settings, a lightweight grid (SG) systems. The plan protected against known security concerns and guaranteed mutual authentication, which was necessary given the complexity and delay-sensitivity of SG networks. BAN logic and the ProVerif tool were used for security validation, which verified the robustness of the system. Performance analysis demonstrated that the scheme proposed by Mahmood et al. [22] achieved the lowest computational and communication overhead compared to existing authentication methods.

Volume 14, Issue 2
April 2025

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

Scheme	Application	Key Focus	Cryptographic Technique(s)	Security Focus	Challenges Addressed	Efficiency/Benefits
IBAKAS [1]	CWSNs	Mutual authentication	IBC, ECC	Authentication, key agreement	Resource constraints, computational overhead	Reduced communication cost, secure authentication
FlexCrypt [2]	CWSNs	Adaptive encryption	Lightweight cryptography, dynamic clustering	Attack resistance	Energy constraints, brute-force, MITM attacks	94% improved network lifetime, scalable security
Topology-Authenticated Key Scheme 2 [3]	Wireless Sensor Networks	Hybrid cryptographic security	Hybrid cryptography	Secure key management	Resource constraints, data reliability	Improved security with minimal overhead
Lightweight Authentication [4]	Mobile Ad hoc Sensor Networks	Efficient authentication	Symmetric cryptography	Secure communication	High energy consumption in authentication	98% energy efficiency, reduced message exchanges
PILOT [5]	Mobile Ad hoc Networks	Reliable group communication	Gossip mechanisms, quorum systems	Fault tolerance, multicast security	High communication overhead	Balanced reliability and efficiency
SEGB-AKA [6]	IoT-enabled LTE/LTE-A Networks	Secure group authentication	Group-based AKA	Key secrecy, unlinkability	Network congestion, single key problem	Reduced signaling congestion, improved security
GLARM [7]	3GPP Networks	Lightweight authentication	Group authentication	Scalability, low overhead	Authentication signaling congestion	60% reduction in authentication overhead
Secure RFID [8]	Smart Healthcare	RFID authentication	Vector space approach	Privacy protection	Forgery, tampering risks	Lower computation & communication costs
Lightweight RFID Auth [9]	RFID Systems	Secure mutual authentication	Hash functions, bitwise operations	Confidentiality, forward secrecy	High computational costs	Efficient with minimal computation overhead

Blockchain Biomedical Imaging [10]	Healthcare 4.0	Secure image processing	ECC, ECDH, ECDSA	Privacy, integrity	Cloud security risks	Faster encryption, improved PSNR & MSE
Group-Based IoT Auth [11]	E-health IoT	Lightweight group authentication	ECC	Device authentication	High energy consumption, security risks	Improved energy efficiency & security
IoT Protocol Analysis [12]	IoT Communication	Security evaluation of protocols	CoAP, MQTT, WebSocket	Data integrity, secure transmission	High latency, energy consumption	Optimized QoS for different IoT scenarios
Blockchain IoT Privacy [13]	Smart IoT Systems	Privacy & consensus	Blockchain, AI, Stackelberg Game	Controlled task distribution	Resource allocation & security	Balanced resource use, secure data flow
IoT Security Review [14]	IoT Networks	Security assessment	Cryptography, Microsoft TMT	Secure SDLC	Man-in-the-middle, DoS, replay attacks	Enhanced security lifecycle management
Dynamic Key Management [15]	5G IoT Networks	Adaptive key generation	Lightweight cipher, dynamic keys	Mutual authentication	Key negotiation overhead	Lower communication latency, better security
Secure Vehicular Networks [16]	Vehicular Networks	Key agreement for V2V/V2I	ECC, Asymmetric keys	Secure group communication	Unauthorized vehicle access	Reduces collisions, enhances authentication
EPSLA [17]	V2V Communication	Secure signcryption	Elliptic Curve Signcryption	Privacy, confidentiality	Message forgery, privacy violations	Low computation & communication cost
Mutual Auth for IoVs [18]	Internet of Vehicles	Secure mutual authentication	Cryptographic primitives	Secure key exchange	Scalability, latency issues	Efficient authentication, scalable design
Blockchain V2V Auth [19]	V2V Communication	Secure real-time data exchange	Blockchain, Link Fingerprints	Authentication, adversary detection	High time complexity	Low latency, secure communication
Secure V2V Data [20]	Smart Cities	V2V secure transmission	One-way hash functions	Data integrity, message authentication	High execution time, security threats	Faster execution, reduced storage costs

Volume 14, Issue 2
April 2025

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

Distributed Learning IoVs [21]	Intelligent Transport	Secure data sharing & model training	Federated Learning, Blockchain	Attack detection, secure training	Vehicle mobility, security threats	Enhanced efficiency, accurate threat detection
Smart Grid Auth [22]	Smart Grid Networks	Authentication for delay-sensitive networks	ECC, ProVerif	Mutual authentication	Delay, security threats	Lowest computational & communication overhead

Table 1: Summarizing Protocols.

5. COMMUNICATIONS IN IOT

The Internet of Things (IoT) represents a vast network of interconnected computing components, including sensors, actuators, and various embedded devices that communicate and exchange data over the Internet. These devices can function autonomously, interacting with other systems and users with minimal human intervention. Given that most mobile and IoT devices rely on WiFi for connectivity, it is crucial to examine the impact of low-power wireless communication on enabling Internet Protocol (IP) connectivity in battery-operated devices.

Connectivity plays a vital role in the efficient functioning of an Internet of Things (IoT) system. Since IoT devices constantly exchange data, maintaining reliable and secure communication is crucial. To ensure stable connectivity, multiple communication protocols are often employed within a single IoT setup. These protocols—such as Bluetooth, WiFi, Zigbee, and Z-Wav [37-39]

Akyildiz et al. *Farooq et al.* *Atzori et al.* help address various environmental and operational constraints that IoT devices encounter.

A typical WSN architecture comprises sensor nodes, gateways, and user interfaces, with applications spanning smart homes, precision agriculture, security systems, and healthcare. However, several key inefficiencies must be addressed in WSNs, including network reliability, node density, latency, and efficient data routing. Since most sensor nodes operate on batteries, energy efficiency is a critical factor in extending the network's lifespan. There is an increasing need for decentralized security mechanisms that allow WSN nodes to self-organize and recover from failures.

Various communication protocols, including RFID, Zigbee, WPAN, WiFi, WiMax, LAN, and WAN, are utilized to facilitate connectivity in WSNs and IoT systems. Among the most explored applications of IoT are smart homes, eHealth, agriculture, and mobility, as these technologies enhance daily human activities through automation and remote monitoring. For instance, smart homes integrate various communication technologies to offer improved convenience, safety, and security to residents. In agriculture, WSN-based solutions enhance productivity and quality by enabling precise monitoring and control. However, given that IoT and WSN devices transmit data over communication networks and often interact with third-party systems, privacy and security considerations are paramount. Additionally, efficient energy management in battery-powered devices remains a significant concern, as optimizing power consumption directly impacts the availability and longevity of sensor nodes.

However, these limitations make safeguarding IoT connections a difficult task. Many conventional cryptographic methods are computationally demanding and necessitate large amounts of memory and processing power, which makes them inappropriate for IoT devices with low resources. This is where **lightweight cryptography** becomes essential. Unlike conventional encryption techniques, lightweight cryptographic algorithms are designed to provide strong security while consuming minimal computational resources, making them ideal for low-power IoT environments. These algorithms ensure data confidentiality, integrity, and authentication without overburdening the device's processing capabilities.

Fig 2: Embedded IoT Platforms

To address communication security inefficiencies, standardization bodies such as the **IEEE and IETF** have developed IoT-specific

protocols like **IEEE 802.15.4e, 6LoWPAN, and LoRa**. These protocols not only optimize connectivity for IoT applications [40] Abderrahmane et al. but also integrate security mechanisms that support lightweight cryptography. By incorporating such optimized cryptographic techniques within these protocols, IoT networks can achieve both secure and efficient communication, ultimately enhancing the overall reliability and safety of IoT ecosystems.

6. SECURITY IN IOT DEVICES

Security risks and weaknesses can arise at any level within an IoT system, making cybersecurity a crucial aspect of its implementation and maintenance [33-35]. IoT devices are susceptible to a variety of assaults, such as data breaches where private information may be stolen, altered, or compromised, hardware-related risks like embedded trojans, and network outages that result in denial-of-service (DoS) attacks. IoT systems' performance and stability may be significantly impacted by such security issues, underscoring the necessity of robust safeguards to guarantee their dependability and security.

Security in IoT systems is a multi-faceted challenge that requires addressing various aspects, including data protection, authentication, access control, and resilience against attacks. Implementing strong security measures across all layers of an IoT network can help ensure safe and reliable operation.

As IoT systems continue to expand across various industries, ensuring their security becomes a top priority. These systems handle sensitive data, interact with critical infrastructures, and often operate in environments where cyber threats are a constant concern. To build a secure and reliable IoT ecosystem, several key security requirements must be addressed Babun et al. [25]:

1. Confidentiality

IoT devices are extremely susceptible to data interception and eavesdropping as they commonly send data via wireless networks. To prevent unwanted access to data, only authorized individuals or devices should access critical information. Encryption methods, secure communication protocols, and access control systems must be used.

2. Integrity

Integrity guarantees that data remains unaltered and trustworthy throughout its lifecycle. Cyber-attacks such as data tampering, replay attacks, and malware injections can manipulate IoT-generated data, leading to false information being processed. To prevent this, cryptographic hash functions, digital signatures, and data validation mechanisms should be employed.

3. Availability

Availability ensures that IoT services and devices remain operational without disruption. Attacks like Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) can overload IoT networks, causing devices to become unresponsive. Implementing redundancy, network monitoring, and efficient resource management can help maintain uninterrupted service availability.

4. Authentication

Before allowing access to IoT networks, authentication is essential for confirming the legitimacy of people, devices, and systems. Unauthorized access might result from inadequate authentication procedures, which presents a serious security risk. To build confidence in the IoT ecosystem, robust authentication mechanisms including cryptographic certificates, biometric authentication, and multi-factor authentication (MFA) are required.

5. Access Control

Permissions and limitations are specified for various individuals and devices via access control techniques. Attackers can get illegal privileges and take advantage of system vulnerabilities if access control is inadequate. Access should be restricted according to predetermined regulations using the least-privilege principle, role-based access control (RBAC), and attribute-based access control (ABAC).

6. Non-Repudiation

Non-repudiation makes assurance that the parties involved cannot retract acts taken within an IoT system. This is especially crucial for uses like legal documents and financial transactions. Digital signatures, audit logs, and blockchain-based verification can help establish accountability in IoT networks.

7. Secure Firmware and Software Updates

Many IoT devices operate with outdated firmware, making them vulnerable to security breaches. Ensuring that devices receive secure and authenticated updates is crucial for mitigating newly discovered threats. Implementing over-the-air (OTA) updates, digital signatures, and secure boot mechanisms can help maintain the security of IoT devices over time.

8. Privacy Protection

Since IoT devices often collect personal and sensitive information, privacy protection is a critical requirement. Unauthorized data collection and exposure can lead to serious privacy violations.

9. Secure Communication

Network data sharing is common among IoT devices, thus secure communication is crucial. Inadequate security measures allow attackers to intercept or alter data while it is in transit. Data security is maintained during transmission by utilizing protocols such as

Volume 14, Issue 2
April 2025

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

Secure Sockets Layer (SSL), Transport Layer Security (TLS), and end-to-end encryption.

10. Resilience Against Cyber Attacks

IoT systems must be designed to withstand and recover from security breaches and cyber-attacks. Intrusion detection systems (IDS), anomaly detection algorithms, and self-healing mechanisms can help IoT devices detect and respond to potential threats proactively.

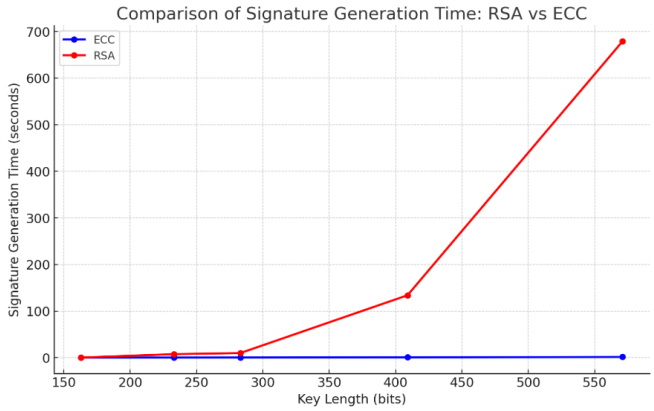

Fig 3: Comparison of key length and computation time for signature generations for RSA and ECC.

7. PRIVACY IN IOT ENVIRONMENT

Privacy is a fundamental human right, making it a top priority in modern application development, particularly in systems that handle user data, the focus here is on how data is processed at the communication level. Despite the numerous benefits of IoT environments,[36] Rosner et al. pose significant risks to human privacy. Many users are unaware of how their personal data is collected, processed, and shared by these systems, while others do not actively safeguard their privacy rights. This lack of awareness affects their understanding of how IoT devices monitor their daily activities and handle sensitive information.

To protect user privacy [26] and prevent unauthorized identification, encrypted communication is crucial for IoT devices. Implementing cryptographic techniques effectively can minimize privacy risks while ensuring secure data transmission. However, Optimizing cryptographic algorithms based on the combination of hardware boards and encryption methods is essential for balancing security with performance. Additionally, evaluating power consumption is vital to maintaining device functionality and extending the lifespan of WSNs, as excessive energy usage can lead to premature device failure, such as battery depletion.

To address these concerns, researchers and Data Protection Authorities (DPAs) have been working on developing and refining data protection frameworks. These frameworks are continuously updated worldwide to keep pace with technological advancements and ensure better privacy protection. Some of the most widely recognized frameworks include the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States.

Key principles of these regulations include:

- **Transparency:** Users should have clear visibility into how their data is accessed, processed, and shared with third parties.
- **Informed Consent:** Individuals must have the ability to provide explicit consent before their data is collected and processed.
- **User Notifications:** Users should be informed about any activities involving their personal data, ensuring they remain aware of how their information is being used.

These regulations aim to enhance user control over personal data while promoting ethical data-handling practices in IoT environments.

8.ISSUES AND CHALLENGES IN LIGHTWEIGHT CRYPTOGRAPHY FOR IOT NETWORKS

Lightweight cryptography is crucial for securing IoT networks, where devices often have limited resources such as low processing power, memory, and battery life. However, implementing secure cryptographic mechanisms in IoT environments comes with several barriers:

1. Limited Computational Power

Most IoT devices have constrained hardware with low processing capabilities, making it difficult to implement standard cryptographic algorithms such as RSA or AES. Lightweight cryptography needs to balance security with minimal computational overhead.

2. Low Energy Availability

Many IoT devices run on batteries and are expected to function for extended periods without frequent recharging. Traditional cryptographic operations can drain battery power quickly, so encryption methods must be energy-efficient.

3. Memory and Storage Constraints

IoT devices often have minimal memory and storage, limiting their ability to store cryptographic keys, certificates, or execute complex encryption schemes. Lightweight cryptographic protocols must be optimized to use minimal memory while ensuring security.

4. Key Management Complexity

Volume 14, Issue 2
April 2025

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

Managing cryptographic keys in large-scale IoT networks is challenging due to the vast number of connected devices. Secure key distribution, renewal, and revocation must be lightweight and efficient while maintaining high security.

5. Real-Time Processing Requirements

Many IoT applications require real-time data processing, such as in healthcare, industrial automation, and smart transportation. Encryption and decryption processes should not introduce significant latency, which could impact the performance of time-sensitive applications.

6. Vulnerability to Side-Channel Attacks

IoT devices are often exposed to physical threats, making them susceptible to side-channel attacks like power analysis, timing attacks, and electromagnetic analysis. Lightweight cryptography must include countermeasures to mitigate these risks.

7. Secure Communication Over Untrusted Networks

IoT devices frequently communicate over public or unsecured networks, increasing the risk of eavesdropping, data tampering, and man-in-the-middle (MITM) attacks. Lightweight cryptographic protocols must ensure end-to-end security with minimal overhead.

8. Scalability Issues

As IoT networks grow, the cryptographic system must scale efficiently to accommodate thousands or even millions of devices while maintaining performance and security. Many traditional cryptographic mechanisms struggle with large-scale deployment.

9. Heterogeneity in IoT Devices

IoT ecosystems consist of diverse devices with different hardware specifications, operating systems, and communication protocols. A one-size-fits-all cryptographic approach is not feasible, requiring adaptable and interoperable security solutions.

10. Standardization and Compatibility

The lack of universal standards for lightweight cryptography creates uncertainties in interoperability between different IoT devices and platforms. Standardized cryptographic frameworks are needed to ensure security while maintaining cross-platform compatibility.

11. Balancing Security and Performance

Achieving a balance between strong security and lightweight performance is a constant challenge. If security mechanisms are too weak, they become ineffective; if they are too strong, they may overwhelm IoT devices' limited resources.

12. Resistance Against Quantum Computing

With the advancement of quantum computing, traditional cryptographic algorithms may become vulnerable. Research is needed to develop lightweight post-quantum cryptography that can be efficiently implemented in IoT devices.

9. IOT SOLUTIONS

The Internet of Things (IoT) goes beyond just being a network of connected devices. Simply linking devices together does not automatically ensure that they function as intended or achieve the desired objectives. For an IoT system to operate effectively, it requires synchronization between multiple components, including IoT devices, cloud servers, specialized applications, communication protocols, and data processing mechanisms. These elements work together to form what is known as an IoT solution—a term that encompasses the integration of all necessary components required for seamless IoT functionality.

An effective IoT solution is more than just a collection of connected devices; it requires a well-structured multi-layered architecture that integrates IoT devices, communication technologies, data processing mechanisms, and user-friendly applications. By understanding the four key layers of an IoT system, researchers and developers can design more efficient, secure, and scalable IoT solutions tailored to various industries and applications.

A fully functional IoT solution consists of four interdependent layers:

1. Sensing Layer
2. Network Layer
3. Data Processing Layer
4. Application Layer

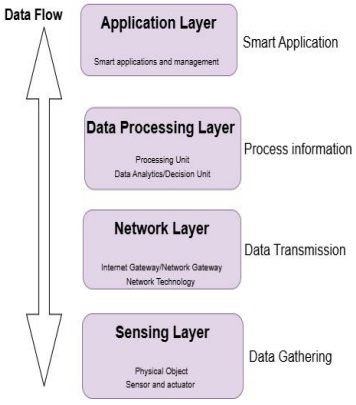

Fig 4: IOT Architecture

Each of these layers plays a critical role in the overall performance of an IoT system.

Volume 14, Issue 2
April 2025

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

1. Sensing Layer

Sensors and actuators that communicate with the real world are among the IoT devices that form the core of an IoT system. Actuators react to real-world input by initiating certain activities, while sensors gather data on motion, temperature, humidity, and pressure. A smart home system's motion sensor, for instance, recognizes movement and tells the smart light to switch on automatically. Whether the IoT system is utilized in smart cities, healthcare, agriculture, or industrial automation, the selection of sensors and actuators is contingent upon the particular use case.

2. Network Layer

The next layer ensures reliable communication between IoT devices and cloud systems. Communication protocols enable seamless data transfer across the network, allowing devices to share information efficiently. Traditional communication technologies like WiFi and Bluetooth were initially used in IoT systems. However, due to the unique requirements of IoT—such as low power consumption, extended range, and the need for device-to-device communication—new specialized protocols have been introduced. ZigBee and Z-Wave, for instance, are designed specifically for IoT applications, offering low-energy consumption, scalability, and reliability. These protocols play a crucial role in enabling IoT devices to remain connected while conserving battery power.

3. Data Processing Layer

Following transmission through communication protocols, data must be processed and analysed. The data processing layer is in charge of filtering, analysing, and interpreting the massive volumes of data produced by IoT devices. This layer frequently incorporates cloud computing or edge computing technologies to process data in real-time or almost real-time. In IoT applications where prompt responses are necessary, like industrial automation or healthcare monitoring systems, effective data processing is essential. The data gathered by sensors must be converted into insightful information to facilitate automation and intelligent decision-making.

4. Application Layer

At the topmost layer of an IoT solution is the IoT application layer. This is where users interact with the IoT system through web interfaces, mobile applications, or dashboards. IoT applications provide users with real-time monitoring, remote control, and automation features. For example, a smart home application allows users to control lighting, temperature, and security systems through a smartphone. Additionally, IoT applications play a vital role in industries such as agriculture, healthcare, and manufacturing, where data visualization and predictive analytics are used to improve efficiency and decision-making.

10. Future Research Directions in IoT Security

1. Privacy Protection in IoT
The issue of privacy protection in IoT is still an emerging area that requires significant research. Due to the vast amount of sensitive data exchanged between IoT devices, ensuring privacy is a crucial challenge, particularly in resource-constrained environments. Many existing security mechanisms are too complex or computationally expensive for lightweight IoT devices, such as sensors and embedded systems. Therefore, future research should focus on developing efficient, lightweight, and secure privacy-preserving techniques that can function effectively in these limited-resource environments. [24]. This will involve novel cryptographic methods, anonymization techniques, and secure data-sharing frameworks that can ensure confidentiality without overburdening IoT devices.

2. Identity Management (IdM) for IoT Devices
As IoT networks expand, managing identities and authorizations for interconnected devices will become increasingly complex. Traditional identity management (IdM) solutions are often not suitable for IoT due to constraints such as limited processing power and memory. Future research should explore the design and deployment of efficient IdM systems specifically tailored for resource-constrained IoT devices. One promising direction is the use of privacy-preserving authentication mechanisms such as Idemix, which enables anonymous credential management while ensuring security. Research in this area should also investigate ways to securely manage machine-to-machine (M2M) authentication and authorization, ensuring that only trusted devices can communicate within an IoT ecosystem.

3. Lightweight Intrusion Detection Systems (IDS) for IoT Security
Security threats in IoT networks can come in various forms, including passive attacks (e.g., eavesdropping) and active attacks (e.g., malicious packet injection and data tampering). Intrusion Detection Systems (IDS) play a crucial role in identifying suspicious activities and mitigating cyber threats. However, conventional IDS mechanisms require significant computational resources, making them unsuitable for IoT environments with constrained power and processing capabilities. Future research should focus on developing lightweight IDS solutions that can detect intrusions efficiently while consuming minimal energy. These IDS should incorporate advanced techniques such as machine learning, behavioural analysis, and anomaly detection to identify potential security breaches in real-time without introducing excessive computational overhead.

4. IoT Security in Healthcare Applications
The integration of IoT in healthcare is revolutionizing patient monitoring and medical data collection.

Technologies such as Wireless Body Area Networks (WBANs)[31-32] He et al. , Ghanavati et al. allow healthcare providers to remotely track patients' vital signs in real-time, improving medical diagnostics and treatment outcomes. However, the transmission of sensitive health data over IoT networks poses significant security and privacy risks. Future research should focus on developing secure and lightweight authentication mechanisms to protect device-to-device (D2D) communication in medical IoT applications. Ensuring the confidentiality and integrity of patient data is critical, and research should explore novel cryptographic techniques that provide strong security while maintaining energy efficiency in healthcare IoT devices.

By addressing these research gaps, future advancements in IoT security will help create a more secure and privacy-preserving IoT ecosystem, ensuring the safe and efficient operation of IoT applications across various domains.

CONCLUSIONS

As IoT devices continue to gain widespread adoption, various companies are developing advanced platforms to facilitate communication between IoT systems and users. These platforms primarily serve to collect, process, and analyze sensor data while automating tasks and executing commands in real time. Despite their differences in functionality and target applications, all IoT platforms must conform to fundamental architectural and programming principles to ensure efficiency and security.

While significant advancements have been made in IoT security, there is still a pressing need for further research and development. A fundamental security requirement for modern IoT platforms is implementing fine-grained access control, ensuring that all entities—including users and devices—have individualized authentication and permissions at every layer of an IoT system. Additionally, areas such as tamper-resistant hardware, IoT application security analysis, device discovery, prevention of data leaks, and vulnerability assessment remain critical topics for future research in IoT security and privacy. Strengthening these aspects will be crucial to building a more secure and resilient IoT ecosystem.

REFERENCES

[1] Mezrag, Fares, Salim Bitam, and Abdelhamid Mellouk. "An efficient and lightweight identity-based scheme for secure communication in clustered wireless sensor networks." Journal of Network and Computer Applications 200 (2022): 103282.

[2] Khashan, Osama A., Rami Ahmad, and Nour M. Khafajah. "An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks." Ad Hoc Networks 115 (2021): 102448.

[3] Tiberti, Walter, et al. "Development of an extended topology-based lightweight cryptographic scheme for IEEE 802.15. 4 wireless sensor networks." International Journal of Distributed Sensor Networks 16.10 (2020): 1550147720951673.

[4] Delgado-Mohatar, Oscar, Amparo Fúster-Sabater, and José M. Sierra. "A light-weight authentication scheme for wireless sensor networks." Ad Hoc Networks 9.5 (2011): 727-735.

[5] Luo, Jun, Patrick Th Eugster, and J-P. Hubaux. "Pilot: Probabilistic lightweight group communication system for ad hoc networks." IEEE transactions on mobile computing 3.2 (2004): 164-179.

[6] Parne, Balu L., Shubham Gupta, and Narendra S. Chaudhari. "Segb: Security enhanced group based aka protocol for m2m communication in an iot enabled lte/lte-a network." IEEE Access 6 (2018): 3668-3684.

[7] Lai, Chengzhe, et al. "GLARM: Group-based lightweight authentication scheme for resource-constrained machine to machine communications." Computer Networks 99 (2016): 66-81.

[8] Shariq, Mohd, and Karan Singh. "A secure and lightweight RFID-enabled protocol for IoT healthcare environment: A vector space based approach." Wireless Personal Communications 127.4 (2022): 3467-3491.

[9] Tewari, Aakanksha, and Brij B. Gupta. "A lightweight mutual authentication approach for RFID tags in IoT devices." International Journal of Networking and Virtual Organisations 18.2 (2018): 97-111.

[10] Rosner, Gilad, and Erin Kenneally. "Clearly opaque: Privacy risks of the internet of things." Rosner, Gilad and Kenneally, Erin, Clearly Opaque: Privacy Risks of the Internet of Things (May 1, 2018). IoT Privacy Forum. 2018.

[11] Almulhim, Maria, Nazurl Islam, and Noor Zaman. "A lightweight and secure authentication scheme for IoT based e-health applications." International Journal of Computer Science and Network Security 19.1 (2019): 107-120.

[12] Bayılmış, Cüneyt, et al. "A survey on communication protocols and performance evaluations for Internet of Things." Digital Communications and Networks 8.6 (2022): 1094-1104.

[13] Han, Daoqi, et al. "Game-theoretic private blockchain design in edge computing networks." Digital Communications and Networks 10.6 (2024): 1622-1634.

[14] Rao, Vidya, and K. V. Prema. "A review on lightweight cryptography for Internet-of-Things based applications." Journal of Ambient Intelligence and Humanized Computing 12.9 (2021): 8835-8857.

[15] Pothumarti, Raghu, Kurunandan Jain, and Prabhakar Krishnan. "A lightweight authentication scheme for 5G mobile communications: a dynamic key approach." Journal of Ambient Intelligence and Humanized Computing (2021): 1-19.

[16] Hsieh, Meng-Yen, et al. "Secure protocols for data propagation and group communication in vehicular networks." EURASIP Journal on Wireless Communications and Networking 2011 (2011): 1-16.

[17] Shao, Huishuang, and Changhao Piao. "A provably secure lightweight authentication based on elliptic curve signcryption for vehicle-to-vehicle communication in vanets." IEEE Transactions on Industrial Informatics 20.3 (2023): 3738-3747.

[18] Vasudev, Harsha, et al. "A lightweight mutual authentication protocol for V2V communication in internet of vehicles." IEEE Transactions on Vehicular Technology 69.6 (2020): 6709-6717.

[19] Kamal, Mohsin, Gautam Srivastava, and Muhammad Tariq. "Blockchain-based lightweight and secured v2v communication in the internet of vehicles." IEEE Transactions on Intelligent Transportation Systems 22.7 (2020): 3997-4004.

[20] Limbasiya, Trupil, and Debasis Das. "Lightweight secure message broadcasting protocol for vehicle-to-vehicle communication." IEEE Systems Journal 14.1 (2019): 520-529.

[21] Huang, Xiaoge, et al. "DAG-based swarm learning: A secure asynchronous learning framework for internet of vehicles." Digital Communications and Networks (2023).

[22] Mahmood, Khalid, et al. "An elliptic curve cryptography based lightweight authentication scheme for smart grid communication." Future Generation Computer Systems 81 (2018): 557-565.

[25] Babun, Leonardo, et al. "A survey on IoT platforms: Communication, security, and privacy perspectives." Computer Networks 192 (2021): 108040.

[26] Silva, Catarina, et al. "Analysis of the cryptographic algorithms in IoT communications." Information Systems Frontiers 26.4 (2024): 1243-1260.

[27] Shaheen, Yaqin, Miguel J. Hornos, and Carlos Rodríguez-Domínguez. "IoT security and privacy challenges from the developer perspective." International Symposium on Ambient Intelligence. Cham: Springer Nature Switzerland, 2023.

[28] Celik, Z. Berkay, et al. "Program analysis of commodity IoT applications for security and privacy: Challenges and opportunities." ACM Computing Surveys (CSUR) 52.4 (2019): 1-30.).

[29] Celik, Z. Berkay, Patrick McDaniel, and Gang Tan. "Soteria: Automated {IoT} safety and security analysis." 2018 USENIX annual technical conference (USENIX ATC 18). 2018.

[30] Celik, Z. Berkay, Gang Tan, and Patrick D. McDaniel. "Iotguard: Dynamic enforcement of security and safety policy in commodity IoT." NDSS. 2019.

[31] He, Debiao, and Sherali Zeadally. "Authentication protocol for an ambient assisted living system." IEEE Communications Magazine 53.1 (2015): 71-77.

[32] Ghanavati, Sara, et al. "Cloud-assisted IoT-based health status monitoring framework." Cluster Computing 20 (2017): 1843-1853.

[33] Meneghello, Francesca, et al. "IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices." IEEE Internet of Things Journal 6.5 (2019): 8182-8201.

[34] Ferrag, Mohamed Amine, et al. "Security and privacy for green IoT-based agriculture: Review, blockchain solutions, and challenges." IEEE access 8 (2020): 32031-32053.

[35] Arias, Orlando, et al. "Privacy and security in internet of things and wearable devices." IEEE transactions on multi-scale computing systems 1.2 (2015): 99-109.

[36] Rosner, Gilad, and Erin Kenneally. "Clearly opaque: Privacy risks of the internet of things." Rosner, Gilad and Kenneally, Erin, Clearly Opaque: Privacy Risks of the Internet of Things (May 1, 2018). IoT Privacy Forum. 2018.

[37] Akyildiz, Ian F., and Josep Miquel Jornet. "The internet of nano-things." IEEE Wireless Communications 17.6 (2010): 58-63.- Discusses IoT communication paradigms and network architectures

[38] Farooq, M. U., et al. "A review on Internet of Things." International Journal of Computer Applications, ISSN 0975 (2015): 8887. an overview of IoT communication protocols, including Bluetooth, WiFi, Zigbee, and Z-Wave.

[39] Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." Computer networks 54.15 (2010): 2787-2805. - communication technologies in IoT systems

[40] Abderrahmane, Tamali, Amardjia Nourredine, and Tamali Mohammed. "Experimental analysis for comparison of wireless transmission technologies: Wi-Fi, Bluetooth, ZigBee and LoRa for mobile multi-robot in hostile sites." International Journal of Electrical and Computer Engineering (IJECE) 14.3 (2024): 2753-2761.

AUTHOR PROFILES

Kamakshi Gupta holds a Bachelor's degree in Computer Science and Engineering from Dr. A.P.J. Abdul Kalam Technical University (AKTU) and a Master's degree in Technology from Guru Gobind

Singh Indraprastha University (GGSIPU), a State University in Dwarka, Delhi, India. She is currently pursuing her Ph.D. at Jamia Millia Islamia, a Central University in New Delhi, India. Her research primarily focuses on cryptography, with a particular interest in lightweight cryptographic protocols tailored for secure communication in the Internet of Things (IoT). Her academic pursuits are driven by a commitment to enhancing security in resource-constrained environments, with broader interests in network security and data privacy.

Prof. Syed Afzal Murtaza (SAM) Rizvi holds a Ph.D. in Computer Science and Engineering and is currently serving as Professor, Department of Computer Science at Jamia Millia Islamia, a Central University in New Delhi, India. With an illustrious academic career spanning over more than 35 years, Prof. Rizvi has demonstrated exceptional commitment to teaching, research, and academic leadership. His expertise extends to course design and academic program development, contributing actively as a member of Boards of Studies and other academic committees. Prof. Rizvi is renowned for fostering IT-driven, interactive learning environments and for building academic programs from inception to advanced levels of excellence.