Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2025 SCPE. Volume 26, Issues 5, pp. 2165–2183, DOI 10.12694/scpe.v26i5.4909

A NOVEL IOT FRAMEWORK FOR IDENTIFYING AND MITIGATING SECURITY THREATS

SHRUTI JAISWAL,* HIMANI BANSAL,† SHIV NARESH SHIVHARE,‡ AND GULSHAN SHRIVASTAVA§

Abstract. The popularity of Internet of Things (IoT) devices has surged due to their applications in diverse areas such as e-Health, smart vehicles, and smart cities. However, the rapid deployment of these devices has led to an exponential increase in security attacks targeting IoT systems, making security a prime concern for the community. Securing IoT-based systems is challenging because the devices involved are often resource-constrained. Providing security to these systems requires a thorough understanding of their specific security needs, along with a systematic security engineering approach. Previous research lacks a systematic methodology for identifying and implementing security requirements. Therefore, there is a growing demand for a structured approach to identify security requirements, select appropriate algorithms, and ensure their effective implementation. While existing studies have extensively explored IoT security threats, they fall short of offering a structured method to comprehensively address these threats. This paper proposes a comprehensive security engineering framework that systematically identifies security threats by analyzing assets present over various layers of IoT system, considering their diverse roles. It includes creating repositories to identify potential vulnerabilities and applicable threats. Once threats are identified, they are evaluated for their severity level based on risk analysis. Following this, the framework focuses on designing the security solutions, where we proposed to add two new security services namely trust and data freshness besides the existing security services, algorithms are selected to mitigate threats by considering the domain and constraints of the devices involved. Ultimately, the security of the entire system is validated to ensure robustness. Throughout this process, we have developed comprehensive repositories for asset management, vulnerability-threat mapping, and algorithm-threat matching to help identify and analyze security needs and recommend algorithms for implementation.

Key words: Internet of Things, security framework, security issues, security algorithms, constraints.

1. Introduction.

The Internet of Things (IoT) is an emerging field that enhances our daily lives by automating routines through the connection of devices and other components via the web. IoT consists of a different physical object forming a network which is surrounded with different type of Sensors/ Actuators, required software's, and a network to provide connectivity and, enabling these objects to gather/ store and exchange data. It enables the remote sensing and control of objects through existing network infrastructure. The concept of IoT extends across various domains, including education, medical, research, home-based automation, industrial, and transport, all of them have a significant impact on our daily lives. It provides a platform for various general household objects to critical jobs at industries to remotely monitor & control various tasks. It would help to improve productivity, ease of usage and information access for promising a better life. There is a steep rise in utilization and connection of devices; providing profitable opportunity for all concerned personswhether the consumer or provider. According to Forbes [1] there are five areas in which IoT is blooming namely, healthcare, Work from home in pandemic times, in retail stores, smart city, amalgamation of edge and IoT devices. According to [2] number of connected IoT devices has grown from 9% to 12.3 billion globally. According to IDC's 2021 U.S. "Smart Home survey on is consumer ready to use smart devices at home for office work, the top most concern of the users of not adopting smart devices for office work is (1) they have not used them before (2) Security and privacy concerns related to their office data and devices" [3].

The growing reliance on IoT has sparked significant concern regarding the study, analysis, and implementation of security measures. As Charles Renert, Vice President of Websense Security Labs, noted, "The Internet of

*Department of CSE&IT, Jaypee Institute of Information Technology, Noida, India (dce.shruti@gmail.com)
†Department of CSE&IT, Jaypee Institute of Information Technology, Noida, India (singal.himani@gmail.com)
‡School of Computer Science Engineering and Technology, Bennett University Greater Noida, Uttar Pradesh-201310, India (shiv827@gmail.com)
§School of Computer Science Engineering and Technology, Bennett University Greater Noida, Uttar Pradesh-201310, India (Corresponding Author, gulshanstv@gmail.com)

Things means consumer products from TVs to refrigerators are now digitally connected. While enterprises may not need to fear interconnected home devices, but every new employee's internet-connected device, application, and upgrade is a potential threat vector" [4]. In recent research, SAP Leonardo has also been used in the IoT domain [39]. This reliance on IoT systems has shifted the focus of the research community towards investigating security aspects. Securing IoT systems is both distinct and challenging compared to traditional network systems due to their layered architecture. Each layer, with its specific devices and constraints, requires a unique focus on security. IoT systems face constraints such as limited on-device memory, reduced computational power, and low energy availability. Researchers detected numerous threats such as eavesdropping and malicious software among others. These incidents on IoT systems have drawn attention from investigators, who are working to address different security aspects to prevent breaches. While a range of methods has been identified to counter these attacks, choosing the most suitable method for a given set of constraints and determining the appropriate algorithm remains a complex challenge.

Numerous researchers have examined the critical need for IoT security and the various criteria that must be addressed. For instance, Hossain et al. [24] and Park and Shin [25] identified key IoT security criteria, including data integrity, information protection, anonymity, non-repudiation, and data freshness. Other studies focus on IoT security concerns within the context of large-scale applications and the broader technological implications of IoT. Schaumont [26] and Jaiswal and Gupta [27], for example, delve into security issues related to IoT-enabled healthcare systems, outlining the challenges and necessary security measures. They emphasize the importance of self-healing, trust, fault tolerance, and lightweight key management protocols, in addition to the standard security requirements such as access control, authentication, and authorization.

Authorization, authentication, confidentiality, access control, trust, and identity management are crucial security requirements for IoT systems, as they are in many other existing systems [28, 29, 30, 31]. Additionally, other general security criteria highlighted in research [32, 33, 34] encompass network security, application security, layer-specific security, data integrity, firewall protection, antivirus capabilities, encryption functions, and secure routing. With the introduction of 5G, IoT security has taken on new challenges. Researchers in [35, 40] have identified several security measures necessary for IoT-based 5G networks. These include authentication, privacy preservation, and ensuring secure communication between devices in the 5G-IoT ecosystem. Given the resource constraints of many IoT devices, they highlight the importance of lightweight cryptographic algorithms. Securing 5G IoT networks is critical because the vast number of interconnected devices increases the potential attack vectors, particularly in high-speed, low-latency networks where real-time data is exchanged. IoT security also extends to data protection techniques, such as encryption. Gupta et al. [36] have proposed a two-level image encryption method specifically designed for IoT devices, addressing the need for lightweight security protocols due to these devices' processing and energy constraints. Their encryption technique offers robust security for IoT systems by employing dual-layer encryption, which is efficient in terms of computational resources while protecting data privacy. As IoT networks grow, they are increasingly integrated with other technologies like fog computing. [37] has reviewed the security challenges in integrating blockchain technology with IoT and fog computing. They identified issues such as scalability, latency, and data integrity in decentralized environments. The study also suggests cell tree solutions to improve the security and efficiency of blockchain-based IoT systems, providing a path forward for secure and scalable IoT implementations.

Numerous researchers are focused on the security aspects of IoT, with some proposing methods to identify threats across different layers of the IoT architecture [5, 6, 7]. In [5], researchers identified potential threats at various layers but did not explore solutions in depth. Another study [7] identified threats at all layers and addressed some inter-layer threats, suggesting broad countermeasures such as encryption and access control. Current proposals mainly emphasize threat identification and suggest mitigation measures like ensuring confidentiality, encrypting data, and providing access control and privacy. However, they often overlook IoT-specific issues such as data freshness and trust, which are critical for the success of IoT systems. Additionally, the IoT domain presents challenges like the need for lightweight algorithms and mobility management. Existing approaches suggest general protection measures but fail to consider domain-specific constraints such as environment, memory, power, and computational speed when selecting security mechanisms like cryptographic algorithms to achieve security objectives like authentication, privacy, and confidentiality. Choosing an algorithm for implementation without accounting domain- specific restrictions can result in an over constrained

system. Thus, an optimal techniques/algorithms should be identified considering domain- specific constraints during the design phase. Moreover, none of the approaches available validate security level, akin to conventional development process, where the software system should be validated for embedded security. This highlights the need for a process that efficiently identifies security threats and guides developers in addressing them effectively.

Providing security to software- based systems is an intricate task, which demands a security engineering method for seamless amalgamation of security concept in software development life cycle. The approach involves starts with identifying, analyzing, prioritizing, and specifying security threats. Then, considering various constraints, the most suitable algorithm for threat mitigation should be selected, followed by validating the system's security level. As a result, a new field known as Security Engineering has emerged, focused on developing processes and methods for applying security in software systems [8]. Ideally, this approach should involve multiple stages of security: (i) requirements, (ii) design, and (iii) testing. This approach should become an integral part of traditional development life cycle model. This paper presents a structured security engineering framework for handling security threats. The process first identifies the generic assets of the IoT system that needs to be protected from intruders. The role played by the assets and possible constraints to assets are identified and stored in repository. Next, the vulnerabilities are identified for assets, and potential threats to these vulnerable points are specified. For mapping of vulnerability corresponding to Assets and Threats corresponding to Vulnerabilities repositories are developed. Next, the risk value for each threat is computed based on occurrence frequency of threat & its impact on assets. Calculation of risk value is required, as we cannot secure the system by 100%. So, risk value would help in knowing which threats need urgent handling and threats which can be ignored. For calculation of impact value, a repository is maintained which contains the assets impacted by threats. Based on the threat's criticality and device constraints, efficient security algorithms is identified for implementation. Security algorithm is chosen based on the threats mitigated and the domain-specific constraints of the selected environment. Different repositories are created and maintained to fulfill the need of developer in an effective way. Once the security algorithm is selected, system security level is tested by calculating security index, which is then compared to pre-defined reference value. If the value of security index is low, we go to selection of algorithm activity again and choose a new algorithm or modify the existing algorithm.

Hence the aim of paper to develop a structured framework which deals with:

1. Identification and categorization of security threats.
2. Selection of security algorithm for mitigation of threats.
3. System security level is evaluated in terms of Security Index.

Rest of the paper is structured as follows: next section provides the overview of security issues in IoT; then the proposal for identification and design of security issues is discussed. After that, a case study is presented to enlighten our proposed framework. Finally, discussion and conclusions with direction of future work is provided.

2. Security Challenges in IoT. The Internet of Things (IoT) integrates a variety of technologies, including networks, cloud systems, transaction management, load balancing, memory management and, many more. Security issues associated with these technologies can impact an IoT system.

Key security issues in IoT systems, include: [3, 6, 7, 8] are:

***Identification / Authentication / Authorization*:** Authentication in IoT is challenging due to the need for heterogeneous network authentication. The identification and authentication of Things must occur before allowing their entry to the network. Each entity in the network requires a unique identification code. Once identified and authenticated, the user must be authorized according to a set of predefined rules.

***Confidentiality & Privacy*:** It's crucial to protect the personal and sensitive data from unauthorized access. Also, private communications must be safeguarded from eavesdroppers.

***Resilience*:** In an IoT system, if an interconnected node is compromised, the system should be able to protect the network, data, and devices from any attacks.

Fault Tolerance: System must continue to work properly with the necessary security services in place, even in the event of a failure.

***Self-Healing*:** In terms of security, self-healing refers to the ability of the network to maintain a minimum level of security even if a sensor or device fails.

***Heterogeneity / Standardization / Interoperability*:** IoT systems consist of a multitude of standalone devices with varying architectures and protocols. The lack of standardization and interoperability among these devices poses significant security challenges, necessitating a robust security design.

***Data Freshness*:** For an IoT network to operate efficiently, nodes must have access to the most recent messages/ information, as these are critical for real-time system performance. For instance, in a patient Surveillance system, a doctor requires the latest ECG readings to assess a patient's heart function.

***Liability*:** There should be accountability in cases of misuse, loss, theft, or unusual events.

***Big Data*:** The communication between devices within an IoT network, as well as with external entities, generates large amounts of data that must be securely managed.

***Constraints*:** Many IoT devices are constrained by limited memory, power, and other resources, making it challenging to implement security measures.

***Trust*:** Trust is essential for users to confidently engage with the system. If users believe the system is secure, they are more likely to use it. However, establishing trust in IoT is difficult due to various security issues.

***Anonymity*:** In some cases, users may wish to remain anonymous.

3. Proposed Security Engineering Process. The proposed security engineering process for identifying and addressing security threats is illustrated in Figure 3.1. Our approach operates in two phases: the first phase involves identifying the various security threats within the system, while the second phase suggests different techniques to mitigate the identified threats based on different design constraints.

Phase I. Identification and Categorization of Threats. In this phase, generic assets, vulnerable points, and threats are identified. Next, the identified threats are assessed to infer their severity, which will further help in selection of security algorithm for implementing threats. Different activities of identification and categorization phase are:

1. *Identify the Assets.* The objective of our research is to secure the system's assets, which can be anything of value to the system, whether tangible or intangible. These assets are central to the system's functionalities and are often targeted by attackers. To address this, a repository of generic assets, categorized by layer, has been designed and maintained to assist developers in selecting the appropriate assets for their systems. This repository was created by analyzing various IoT domains, such as smart homes, e-healthcare, vehicle tracking, and transportation [9, 10, 11, 12, 13]. Additionally, assets are classified by type (where applicable), and any constraints or limitations associated with the assets are also identified. These constraints are crucial when selecting or providing security solutions to mitigate threats within the system. New assets identified during the research are added to the repository for future consideration. Table 3.1 is created to store assets at various IoT layers, along with their constraints and roles.
2. *Identification of Vulnerabilities.* Vulnerabilities are system weaknesses that attackers can exploit to gain access to system resources. Therefore, it's crucial to identify these points to protect system assets from potential attacks. To address the need for vulnerability identification, we developed a repository based on an extensive literature review [4, 13, 14]. A sample repository is depicted in Table 3.2; further details on other vulnerabilities related to assets can be obtained from the author. For clarity and proper reference, "V" prefix is added to vulnerabilities. Vulnerabilities are selected from the maintained repository on the basis of role of the asset of all stakeholders. To facilitate, a scenario diagram is created to illustrate when and how an asset is accessed and used, as depicted in Figure 3.2. Any new vulnerabilities reported are documented for future reference.
3. *Identify the Threats.* To secure system assets, it is essential to understand the potential threats to those assets. Thus, identifying potential threats at various vulnerable points is necessary. To facilitate this, we have proposed a mapping table with dimensions of 39×22, a portion of which is shown in Table 3.3. It illustrates the possible threats at vulnerable points, where an "✓" indicates that a particular threat may occur at a specific vulnerable point. These threats are then identified and extracted from the table using the scenario diagram created in the previous step.
4. *Threat Evaluation.* Evaluation of threats plays an important role as it allows us to measure the severity of probable threats. Risk value for each threat is calculated using the threat occurrence probability

Table 3.1: Assets at various Layers of IoT

S. No.	Layer	Assets	Further Sub-Categorization	Constraints/ Limitations	Role
1	Sensing	Sensors/ Actuators/ Controllers	- Environment Sensors (Light, Temperature, etc.) - Body Sensors (ECG, Blood Pressure, etc.) - Motion detectors - Microphone sensors - Gas/ Smoke detectors - Electrical Current/ ON-OFF Sensors - Door (magnet) Sensors - Physiological sensors	- Limited power - Limited Battery Capacity - Limited memory - Reduced Computational Speed - Limited Bandwidth for Communication	Acquire data
2	Sensing	Labels and Markers	- RFID tags - NFC (Near Field Communication) - Security tokens - Smart cards - SIM cards	- Limited Power - Limited Battery Capacity - Limited memory - Reduced Computational Speed - Limited Bandwidth for Communication	For device identification
3	Sensing	Data repository	- On- premise server - Cloud storage - Removable media	- Large volume of data - No Fixed Structure - Variable structure (Structured, Unstructured) - Sensitive data - Data source - Diverse formats - Availability	For storing large volumes of generated or created data
4	Sensing	Devices	- Home appliances (e.g., Refrigerator, Washing machine) - Hospital equipment (Various machines) - Screen and speakers	- Availability - Environment Limitations - Battery/ Power/ Charging considerations	Appliances used in IoT network
5	Communication	Communication Network	- Internet connection (wired or wireless) - Networking components (e.g., Routers, Bridge)	- Bandwidth limitation based on devices	For efficient communication
6	User Interface	User interface device	- Specialized terminal - Gateway interface - Remote control devices - Smartphones, Smart TVs - Tablets, Desktop computers /PCs - SOS/ Emergency buttons - Set-top box user interfaces - Calendar/ Reminder devices	- Battery/ Power/ charging considerations - Availability - Environment Limitations	Mode of user interaction
7	Between the interface of two Layers	Software Programs	- Operating system(s) - Device drivers - Applications - Firmware	- Auto-update - Security Patch Update - Compatibility - Battery/ Power/ Charging	For Data Processing
8	At each layer	Data/ Information	- Access/ payment credentials to external accounts - Smart setup/ structure/ inventory information - Status information - User preferences - Intellectual property/Value - Security (Passwords, User identifier) - Privacy (User biometrics, Behavioral patterns and trends) - Resources (Music, Audio/ Visual media, Pictures, etc.	- Distributed - Bulky/ Huge - Confidential - Generated from different sources - Different Formats	Crucial and important data for processing
9	Miscellaneous	Physical Resources	- Building infrastructure - Hardware (Air conditioners, Meters, Light, etc.)	- Physical constraints	Provides Infrastructure
10	People/ Users	People/ User	- End users - Providers - Customers	- From a different technical background - May/may not have security knowledge	Access and manage the system

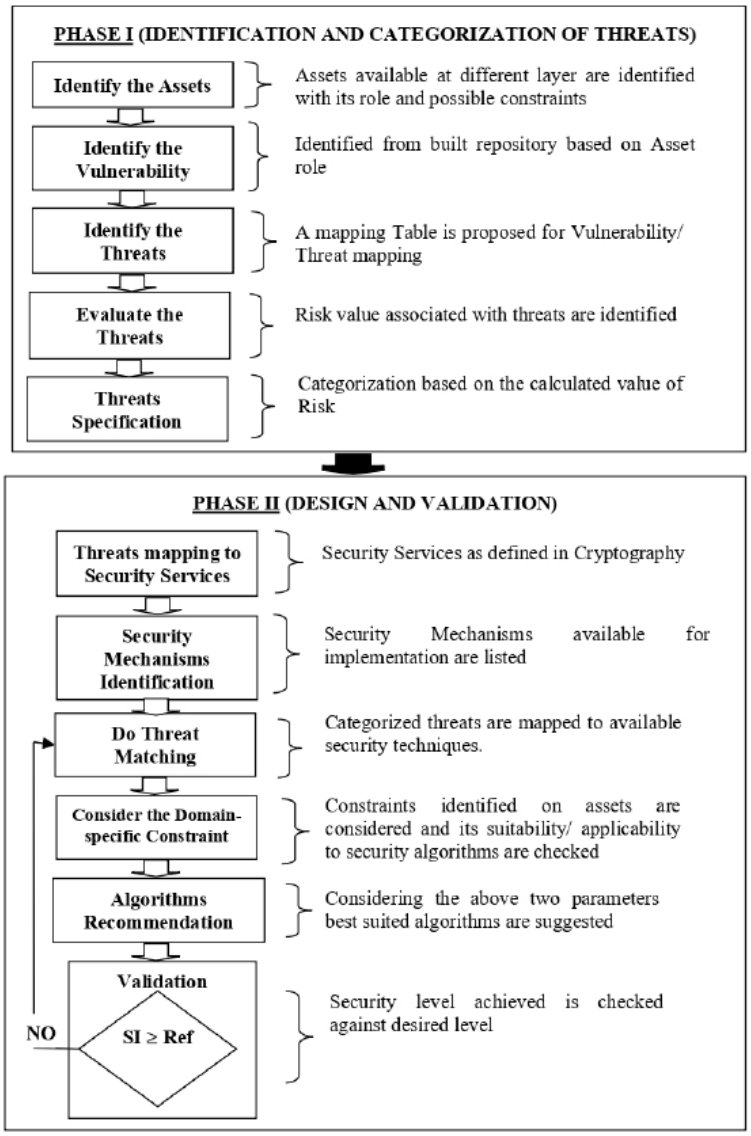

Fig. 3.1: Proposed Framework

and its impact on the system. Prioritization/ evaluation of threats is necessary as most of the projects has constraints, so all threats cannot be mitigated, and the developers need to decide which threats to choose first for implementation. The process followed for prioritization, is shown in Figure 3.3 and explained subsequently:

(a) *Impact Identification:* Impact of occurrence of a threat on the system is identified by examining the number of assets impacted when it occurs. Therefore, it would simply be the summation of impacted assets values represented by Eq. 3.1 as follows:

$$\text{Impact} = \sum \text{Asset rating of impacted assets} \tag{3.1}$$

As impact depends on asset rating, asset rating is required to be calculated. Calculation of asset value is an important task as it shows its importance. In many risk analysis methods,

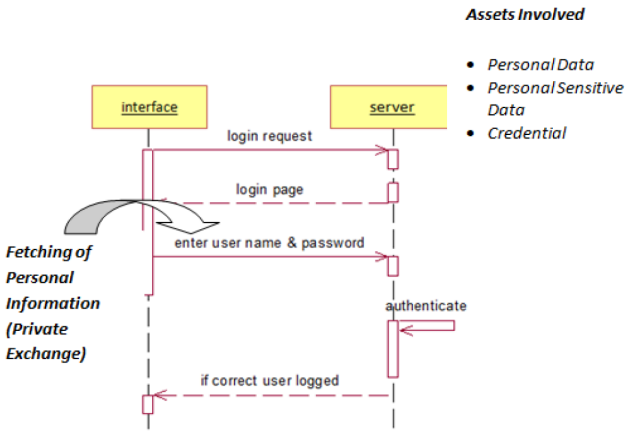

Fig. 3.2: Scenario Diagram for Login functionality

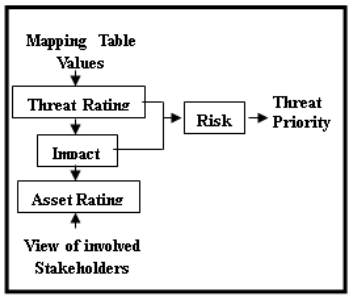

Fig. 3.3: Process for Prioritization of Threats

such as CRAMM [15], CORAS [16], assets are given a rating based on their importance to the system. We propose that assets valuation would be more accurate if it considers the perspectives of all relevant stakeholders. For instance, asset Sensors/ Actuators is evaluated by stakeholders Consumer, Provider, Administrator and Vendor as 8, 9, 7 and 6 respectively. So, by analyzing the views of stakeholders, final asset value using Eq. 3.2 is '8'.

$$\text{Asset Value} = \sum \frac{\text{View of involved actor for Asset}}{\text{Number of actors involved}} \tag{3.2}$$

Impact is calculated by adding the asset rating of impacted assets by threats. Table 3.4 shows the list of assets impacted by occurrence of threat. For instance, suppose threat T. Manipulation of Hardware and Software would impact assets (Sensors/ Actuators, Software, User interface device, Labels and Markers, and Data repository).

(b) *Calculate the Risk:* Risk measures the potential damage that a threat can inflict on the system. As mentioned by OWASP [20],], risk is represented by Eq. 3.3. Using Eq. 3.3 risk value of all identified threats are calculated.

$$\text{Risk} = \text{Threat Rating} \times \text{Impact} \tag{3.3}$$

(c) *Threat Categorization:* Categorization of threats is done to represent threats clearly and precisely, which is done using the identified risk values. Threats are categorized on the basis of following criteria:

Table 3.2: Identified Vulnerabilities for Assets

Assets	Vulnerabilities
Sensors/ Actuators	V. InadequateAccessControl V.UnencryptedData V. LackofPhysicalSecurity V.Misconfiguration V.InsecureInterfaces V.InsufficientSecurityConfigurability V.RemoteAccess V.SystemMisuse V.LackofMonitoring V.InsufficientLogging V.LackofStandards
Software Programs	V.InsufficientLogging V.Misconfigurations V.UnsafeAPIFirmware V.OutdatedSystem V.LackofStandards V.Intrusion Detection

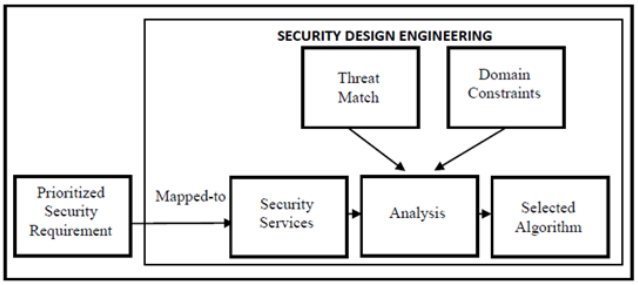

Fig. 3.4: Security design process.

i. If ($Risk \geq 60$), Then Category is Catastrophic, which needs urgent handling because the threats impact various high-value assets.
ii. If ($60 > Risk \geq 20$), Then Category is Important, which require careful consideration because the threats are impacting:
   - Various moderate assets
   - A high-value
iii. If ($20 > Risk \geq 5$), Then Category is Acceptable which can be considered or ignored
iv. If ($Risk < 5$) Then No Effect because low-value assets are impacted, hence can be ignored. Categorized threats are stored for further action.

Categorized threats are stored for further action.

Phase II. Design and Validation. Once threats have been prioritized and categorized, the next phase involves selecting appropriate security algorithms. This selection process focuses on identifying algorithms that effectively address the prioritized threats. The choice of algorithm for implementation is based on: (i) threats it mitigates; (ii) the domain- specific constraints/ limitations of the environment where the algorithm will be implemented. After selecting the necessary algorithms for implementation, testing is conducted to ensure if all threats are adequately addressed. For clear illustration a simplified diagram to depict the design process is shown in Figure 3.4.

Table 3.3: Threat-Vulnerability Mapping Table

Vulnerabilities / Threats	V. Inadequate_Access_Control	V. Insufficient_Logging	V. Penerated_Firewall	V. Unsanitized_Input	V. Unsafe_API_Frimware	V. Outdated_System	V. Misconfiguration	V. Non-Encrypted_Data	V. Naive_User	V. Lack_of_Monitoring	V. Vulnerable_Network	V. Intrusion_Detection	V. Physical_Protection	Threat Rating
T. Identity_Theft	✓	✓							✓					3
T. Infected_e-mail			✓		✓						✓	✓		4
T. Denial_of_Service (DoS)										✓		✓		2
T. Information_Leakage								✓			✓			2
T. . Rouge Certificates Generation and Use	✓	✓												2
T. Manipulation of Software and Hardware														0
T. Information manipulation	✓	✓						✓	✓	✓				5
T. Misuse Audit Tools	✓								✓					2
T. Records Falsification	✓			✓	✓					✓				4
T. Unauthorized use of Administrative Resources	✓	✓												2

1. *Threats Mapping to Security Services:* Threats are associated with major security services CIA triad (Confidentiality, Integrity, Availability), access control, and non-repudiation [17] This mapping will be beneficial in later stages by identifying the appropriate security mechanisms for implementation. Considering, each threat separately is challenging, so mechanisms are categorized according to security services for effective handling of security threats in the system. Besides the already defined security services, two more services are added, namely 'Data Freshness' and 'Trust', which are required to be considered for the IoT domain as several proposals defended the need for data freshness (real-time data) and trust as an integral part of security subsystem [27, 38]. Besides the IoT domain, other emerging areas such as fog, edge, and blockchain are all working on a recent data set; hence, there is a need to include data freshness and make people adopt these emerging technologies; trust should also become an integral part of security services. Threats mapping to security service 'Confidentiality' is shown in Table 3.5.
2. *Security Mechanisms Identification:* Various security algorithms that can be used to implement the system's security services are explored. Table 3.5 provides details for just one security service. Once the available security mechanisms are identified, the design and security teams will analyze the algorithms and select the most suitable mechanism for implementation, following the subsequent activities.
3. *Do Threat Matching:* A repository for analyzing security algorithms is created. The categorized threats are then compared against this repository, and the algorithm that mitigates the most threats is selected. Table 3.6 provides a sample repository for confidentiality. A ✓in the table indicates that the security technique can address the matching threat. For instance, the AES technique under the asymmetric category mitigates threats such as Unauthorized Software use, Unauthorized Software Installation, Communication Breach, MITM attacks, and Violation of Privacy. The last row of the table shows the total impact, indicating the number of threats each technique mitigates. Each value corresponds to the different techniques listed at the top.
4. *Consider the Domain-specific Constraints/ Limitations:* Algorithm choice is based on amount of threats they mitigate, but not all algorithms are suitable for every scenario. Therefore, further analysis of

Table 3.4: Impacted Assets by Threats

Threats	Impacted Assets
T. Rouge Certificates Generation and use	Sensors/ Actuators Software Programs User interface device Data/ Information Labels and Markers Communication Network Data repository Devices
T. Manipulation of Hardware and Software	Sensors/ Actuators Software Programs User interface device Labels and Markers Data repository
T. Failure and Malfunctions	Sensors/ Actuators Software Programs User interface device Physical Resources Labels and Markers Communication Network Data repository Devices
T. Information Leakage	Sensors/ Actuators Physical Resources Labels and Markers Communication Network Data repository

domain constraints/ limitations imposed by devices, the environment, and other factors is conducted. Categorization of domain constraints is shown in Figure 3.5. The selected algorithms are then evaluated based on domain- specific constraints viz. power, memory usage, and more. Table 3.7 illustrates the limitations of the IoT system. In Table 3.7 values varies from minimal to extensive depending on the domain of application.

5. *Algorithm Recommendation:* As previous process of threat matching & consideration of domain- specific constraints, most suitable algorithms are selected for implementation.
6. *Validation:* The validation of chosen algorithm/ mechanism is performed to determine whether the potential threats to the system are effectively mitigated. To cater this, a Security Index (SI) value is considered, which indicates the remaining gap in the system. The SI is defined as the ratio of mitigated threats to the initial number of identified threats, as shown in Eq. 3.4.

$$\text{Security Index} = \frac{\text{Mitigated Threats}}{\text{Identified Threats}} \times 100 \tag{3.4}$$

A high SI value (close to 100) indicates that the system is secure, while a low SI value (approaching 0) suggests that the system is unsafe and requires revisions to the design decisions, particularly the selection of security algorithms. The reference value is defined by the administrator based on the domain of application, level of CIA required, criticality of the system. Its value may change from one system to other based on its domain constraints. If modifications to security are necessary, the developer must return to the beginning of the second phase to choose or adjust the algorithm for implementation.

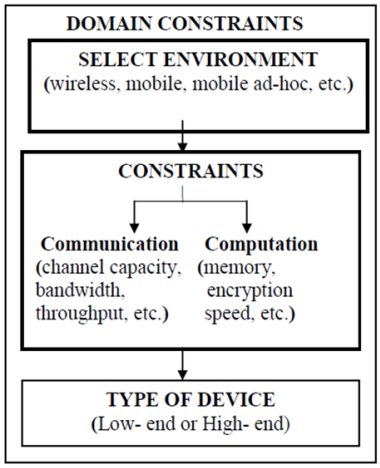

Fig. 3.5: Categorization of Domain Constraints.

Table 3.5: Threats Mapping to Security Services and Mechanism

Security Services	Threats	Security Mechanism Available	Possible Techniques	Techniques Characteristic
Data Confidentiality	T. Unauthorized Software use T. Unauthorized Software Installation T. Compromise of Confidential Information T. Communication Breach T. Eavesdropping T. MITM T. Violation of Privacy T. Rogue Employee T. Identity theft	Encryption, Routing Protocol	**Encryption** **Asymmetric** (AES, DES, Triple DES) **Symmetric** (RSA, Rabin's Scheme, ECC, HECC)	**Asymmetric** – Each node possesses its own unique set of keys – Takes more power due to computational complexity – Good scalability **Symmetric** – Ensures key confidentiality – Complex protocol for key management – Authentication demands higher power consumption – Simple calculations, resulting in lower power consumption
			Routing Protocol (AOMDV-IoT, SMRP, EARA, RPL, Multiparent routing in RPL, PAIR, REL)	Prevent routing attacks like spoofing, sinkhole, and selective forwarding.

4. Case Study: Patient Surveillance System. Healthcare domain is chosen because of the facts given in the report by grand view research [18]:

- The COVID-19 pandemic significantly boosted the IoT in healthcare market by accelerating the adoption of remote patient monitoring and telemedicine. This shift was driven by the need for innovative technologies to manage health data remotely, reducing in-person contact and improving healthcare outcomes.
- The global Internet of Things (IoT) in healthcare market was valued at USD 44.21 billion in 2023 and is projected to grow at a compound annual growth rate (CAGR) of 21.2% from 2024 to 2030

Table 3.6: Mapping of Security Mechanisms to Threats. A1- (AES) Advanced Encryption Standard, A2- (DES) Data Encryption Standard, A3- Triple- DES; S1- RSA (Rivest–Shamir–Adleman), S2- ECC (Elliptic Curve Cryptography), S3- HECC (Hyperelliptic curve cryptography); H1- ECIES (ECIES Hybrid Encryption Scheme)

	Asymmetric			Symmetric			Hybrid
Techniques/Threats	A1	A2	A3	S1	S2	S3	H1
T. Unauthorized Software use	✓	✓	✓	✓	✓	✓	✓
T. Unauthorized Software Installation	✓	✓	✓	✓	✓	✓	✓
T. Compromise of Confidential Information							✓
T. Communication Breach	✓				✓	✓	✓
T. Eavesdropping							✓
T. MITM	✓				✓	✓	✓
T. Violation of Privacy	✓	✓	✓	✓	✓	✓	✓
T. Rogue Employee							✓
T. Identity theft				✓	✓		✓
T. Confidential Data Compromise	✓				✓	✓	✓
T. Credential theft	✓				✓	✓	✓
T. Information Leakage	✓				✓	✓	✓
TOTAL IMPACT	8	3	3	4	9	8	12

Table 3.7: Limitations across various IoT layers

Parameters	Sensing	Communication	User Interface
Parameters related to Performance			
Memory Computation Speed Energy Run Time performance	Minimal, Intermediate, Extensive		
Other Parameters			
Security Objectives Mobility Compatibility Scalability Cost of the chosen solution Portability	Minimal, Intermediate, Extensive		

- The market is fueled by the growing use of smartphones, smart devices, and wearables for patient monitoring. Additionally, the rising adoption of remote patient monitoring to enhance out-of-hospital care further drives market growth.

The Remote Patient Surveillance System illustrated in Figure 4.1 is an integral component of the healthcare system.

1. *Wireless Body Area Network.* This network consists of wearable sensors that can store small amounts of data and transmit it to remote server/ location.
2. *E-Health Gateway.* This component forwards data packets from the WBAN to other networks.
3. *Internet.* The communication network responsible for carrying the information/ data.
4. *Healthcare Data Centre.* This facility stores all the data generated by the sensors in WBAN. Given the large volume of data, proper management is essential.
5. *Medical Service.* Provides medical facilities to patient such as consultations based on regular check-ups and other services.

In the above system, the following actors are considered: Patient, Doctor, and Insurance Service Provider. Each user has different roles and responsibilities; here, we will consider an abstract overview of all roles for

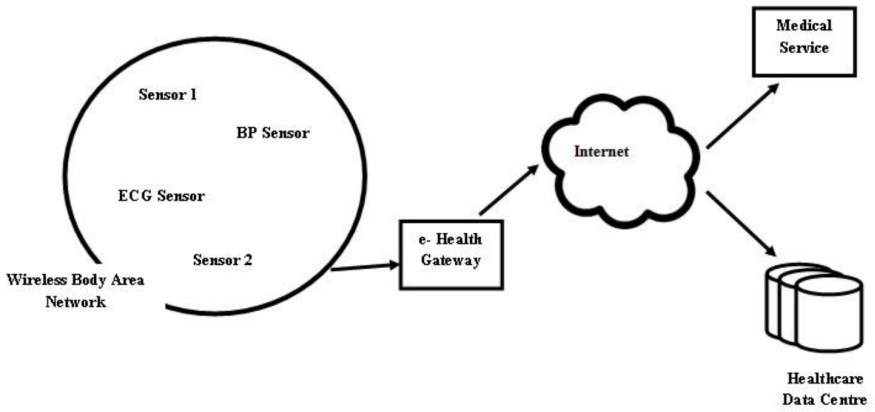

Fig. 4.1: Remote Patient Monitoring System

further explanation.

Phase I. Identification and Categorization.

1. *Identify the Assets.* Patient surveillance has following assets: body sensors, data repository, network and connection components, a smartphone with an application for interaction, and patient information. Each asset plays a specific role, as detailed below:
   - Body Sensors: Attached to the patient's body to monitor physiological parameters and transmit the data to either remote storage or a processing device.
   - Data repository: Store collected data
   - Network and connections: For communication between nodes
   - Smart Phone: For user interaction
   - Patient Information: Personal and health information of the patient available in the system.
2. *Identification of vulnerabilities.* Identified Vulnerabilities are extracted for all assets involved in Remote Patient Surveillance System from repository depicted in Table 3.2 using the scenario diagram. Vulnerabilities extracted for asset:
   (a) *Body Sensors*
      - Inadequate Access Control
      - Unencrypted Data
      - Lack of Physical Security
      - Misconfiguration
      - Insecure Interfaces
      - Insufficient Security Configurability
      - Remote Access

   (b) *Data repository*
      - Inadequate Access Control
      - Insufficient Security Configurability
      - Unencrypted Data
      - Intrusion Detection
      - Misconfigurations
      - Insecure Interfaces
      - System Misuse

   Similarly, vulnerabilities applicable to other assets are identified.
3. *Identify the Threats.* Threats are extracted corresponding to identified vulnerable points for each asset. Threats to asset Body Sensors are:

Table 4.1: Risk Calculation intended for Probable Threats

Threats	Affected Assets	Threat Rating	Impact	Risk
T. Identity theft	Sensors/ Actuators Interface device Data/ Information Communication-Network Data repository	5	40	200
T. DoS	Sensors/ Actuators Data repository	2	17	34
T. Rouge Certificates Generation and use	Sensors/ Actuators Interface device Data/ Information Communication-Network Data repository	5	40	200

- Information manipulation
- Repudiation
- Misuse of Personal Data
- Records Falsification
- Information Leakage
- Physical Attacks
- Compromise of Confidential Information
- Failure and Malfunctions
- Accidental Damages

4. *Evaluate the Threats:* Prioritization of threats is done by considering the impact of threats on the involved assets. Calculation of risk values for our system is presented in Table 4.1.

Assets Evaluation. System assets are evaluated by involved stakeholders, as explained in section 3. For example, involved assets are assessed as:

- Body Sensors as 8
- Interface Device as 8
- Patient Information as 8
- Network and Connections as 7
- Data repository as 9

Threat Categorization. Threats are categorized in the following categories:

1. *Catastrophic:*
   - Identity theft
   - Credential theft
   - Generation and use of Rogue Certificates
   - Records Falsification
   - Unauthorized use of Administrative Resources
   - Unauthorized Software Installation
   - Confidential Data Compromise
   - Replay Message
   - Eavesdropping
   - Violation of Law or Regulations
   - Failure and Malfunctions
   - Accidental Damages
   - Violation of Privacy
   - Fake Node
   - Phishing

- Spoofing
- Information Leakage
- Information manipulation
- Repudiation
- Illegal Access to Information System
- Unauthorized Software use
- Rogue Employee
- Communication Breach
- Misuse of Audit Tools
- MITM
- Infected Email
- Malware
- Human Error

2. *Important:*
   - DoS
   - Hardware Failure
   - Misuse of Personal Data
   - Loss of Support Services
3. *Acceptable:*
   - Physical Attacks
   - Natural Calamity
   - Environmental Calamity
   - Node Capture
4. *No Effect:* Nil

Phase II. Handling.

1. Threats Mapping to Security Services. Table 3.5 shows mapping of threats to security services.
2. Security Mechanisms Identification. Security mechanisms available for implementation are listed in Table 3.5.
3. Algorithms Recommendation. Based on the threat matches (as shown in Table 3.6) and system limitations (as shown in Table 4.2), suitable algorithms are recommended for implementation. Table 3.6 is built for algorithms related to threats to confidentiality. Here, for explanation purposes, only the confidentiality part is emphasized in detail during the validation part. Other algorithms are chosen based on the domain of the application and its constraints. As the Patient Surveillance System, we have memory, power, and speed constraint hybrid algorithm ECIES, which is more suitable as it requires less power than AES and ECC algorithms and can mitigate a maximum number of threats.
   - Encryption
     a) Asymmetric Encryption Algorithm: AES
     b) Symmetric Encryption Algorithm: ECC
     c) Hybrid Algorithm: ECIES
   - Routing Control: Energy-aware Ant Routing Algorithm (EARA)
   - Authentication Exchanges: Two Step Authentication
   - Data Integrity: MD5
   - Digital Signature: ECDSA
   - Access Control Mechanism: Role-Based Access Control
   - Notarization: Establish a Notary Server
   - Physical Protection Mechanisms: Locks, Physical Security Guards
4. Validation to ensuring Confidentiality Identified threats related security service confidentiality:
   - Identity theft
   - Records Falsification
   - Unauthorized Software Installation
   - Confidential Data Compromise

Table 4.2: Constraint to different Layers for Remote Patient Surveillance System

Parameter	Sensing	Communication	User Interface
Parameters related to Performance			
Memory	Minimal	Intermediate	Extensive
Computation Speed	Minimal	Intermediate	Extensive
Energy / Power	Minimal	Intermediate-Extensive	Extensive
Run Time performance	Intermediate	Extensive	Extensive
Other Parameters			
Security Objectives	Extensive	Extensive	Extensive
Mobility Compatibility	Extensive	Extensive	Extensive
Scalability	Minimal	Extensive	Extensive
Cost of the chosen solution	Minimal	Minimal	Minimal
Portability	Extensive	Extensive	Extensive

- Credential theft
- Eavesdropping
- Violation of Privacy
- Information manipulation
- Information Leakage
- Unauthorized Software use
- Communication Breach
- MITM

Referring to Table 3.6, threats matching is done, and SI value is calculated for threats pertaining to confidentiality.

Asymmetric Algorithm. AES is selected. Security Index = $\frac{7}{12} \times 100 = 58.33\%$

Symmetric Algorithm. ECC is selected. Security Index = $\frac{8}{12} \times 100 = 66.67\%$. However, neither of the algorithms alone provides adequate protection, so hybrid techniques are necessary. Therefore, the hybrid technique ECIES has been selected. The Security Index (SI) is calculated as SI = $\frac{10}{12} \times 100 = 83.33\%$. While the hybrid algorithm significantly improves upon the existing algorithms, additional algorithms are needed for optimal effectiveness.

5. Discussion. Current proposals only specify the threats and do not have steps for prioritization and categorization. However, none of the existing approaches recommend a specific security algorithm for implementation. They only specify the broad implementation measures that are architectural constraints, and checking the system's security level is not discussed.

The process from threat elicitation to prioritization for IoT systems is outlined. In this method, assets and potential threats to them were identified alongside system functionalities. After prioritizing the identified threats, they are classified into categories such as catastrophic and significant. Security algorithms are chosen based on domain-specific limitations, including being lightweight (i.e., consuming less power and requiring minimal computation time) and having low storage requirements. Ultimately, a metric is developed to reflect the system's security level. This approach is illustrated within the context of IoT-enabled medical care, particularly for remote patient surveillance.

To achieve these objectives, the following activities are carried out:

- Identification of assets across various IoT layers, along with their potential threats and vulnerabilities.
- Creation of a threat repository affecting system assets, with dimensions of 39×30.
- Suggestion of security mechanisms based on domain constraints.

The high Security Index result indicates that existing security algorithms are insufficient, necessitating the development of new algorithms. Our approach differs from previous techniques by providing a structured process for incorporating security into software systems. A comparison of this with existing approaches is shown

Table 5.1: Comparison of our proposal with existing literature.

Method	Domain	Key Contributions	Challenges Highlighted	Proposed Solutions/Frameworks
Hossain et al. [24]	IoT Security Challenges and Approaches	Meta-study on IoT security challenges, approaches, and open issues	Scalability, privacy, resource constraints	Discusses various security approaches, open research areas
Park and Shin [25]	IoT Security Assessment Framework	Proposes a framework for assessing security in IoT services	Heterogeneous device security, privacy	Framework for systematic security assessment in IoT services
Schaumont [26]	Scale Challenges in IoT Security	Discusses the unique challenge of scaling security across numerous IoT devices	Scalability, energy efficiency	Suggests scalable security mechanisms appropriate for large IoT networks
Jaiswal and Gupta [27]	IoT Security Requirements	Identifies essential security requirements for IoT systems	Data integrity, user privacy, access control	Emphasizes the need for comprehensive IoT security models
Tourani et al. [28]	Security, Privacy, and Access Control in IoT	Surveys security, privacy, and access control in IoT-based networks	Privacy, access control, secure data management	Provides a taxonomy of IoT security approaches and open challenges
Zhou et al. [29]	IoT New Features and Security Impact	Examines how IoT-specific features affect security and privacy	New vulnerabilities due to IoT features	Discusses existing solutions and gaps addressing IoT-specific security
Ammar et al. [30]	Security in IoT Frameworks	Surveys security in existing IoT frameworks	Data security, interoperability, scalability	Reviews security methods within various IoT frameworks
Asiri [31]	Blockchain in IoT	Proposes a blockchain-based trust model for IoT	Trust, decentralization	Blockchain-based model for enhancing trust in IoT environments
Jerald et al. [32]	Secure IoT Architecture	Proposes a secure architecture for smart services in IoT	Integration of multiple smart services securely	A secure architecture framework for smart IoT environments
Sedrati and Mezrioui [33]	IoT Security Challenges	Overview of IoT security with a focus on challenges	Data breaches, device vulnerabilities	Highlights the need for adaptive security measures in IoT
Oracevic et al. [34]	IoT Security Survey	A general survey of IoT security	Device security, secure communication, data privacy	Consolidates existing approaches to IoT security
Dey et al. [35]	IoT Security in 5G Networks	Focus on security measures in IoT within 5G networks	Network slicing, data integrity	Recommends security approaches tailored to IoT in 5G
Gupta et al. [36]	Image Encryption for IoT	Proposes a two-level image encryption for IoT	Data protection, secure communication	Two-level encryption for secure image transmission in IoT
Khan and Chishti [37]	Fog and IoT Security	Discusses challenges and solutions for IoT in fog computing and blockchain	Scalability, data privacy	Reviews fog-based and blockchain solutions for IoT
Pal et al. [38]	Systematic Approach to IoT Security Requirements	Systematic review of IoT security requirements	Authentication, integrity, privacy	Framework for structured analysis of IoT security needs
Proposed Approach	Systematic Approach for Identification and Mitigation of threats by recommending appropriate security algorithms for implementation	Creation of different databases for assets available at each layer, vulnerability and threats mapping table, and design constraints related to IoT system	Addition of new security requirements, recommendation of hybrid algorithm for implementation	Structured framework of security engineering for IoT-based system

in Table 5.1. Our approach can be adopted for emerging IoT areas by exploring the vulnerabilities and threats specific to that area, if any. If a new vulnerability or threat is found, we need to just extend our database by adding its related information. By doing this, we can adapt our framework for any related domain.

6. Conclusion and Future Work. A structured framework for incorporating security in IoT-based systems is projected. This framework identifies and categorizes threats to security, and selects efficient security algorithms for implementation based on the threats mitigated and domain constraints.

The novel contributions of our work are:

- Elicitation, analysis, prioritization, and categorization of threats to assets.
- New security services were added namely data freshness and trust.
- During requirements engineering phase, probable threats to assets are identified. To support threat elicitation, we have created:
  - i A repository of assets for IoT architecture.
  - ii A vulnerability threat mapping table with dimensions of 39×22.
  - iii A table of threats affecting system assets, with approx. dimension of 39×30 is prepared. It helps in managing different assets, functionalities, threats, and vulnerabilities.
- Selection of algorithms to implement security in system is based on domain- specific constraints across different layers of IoT.
- Generation of a security metric to indicate the system's security.
- In the context of Patient Surveillance System, a hybrid algorithm is proposed to meet security requirements.

In future, we plan to conduct a thorough analysis of the computational overhead versus the security benefits essential for selecting new algorithms over traditional ones. We also aim to explore combinations of threats and vulnerabilities that could potentially lead to new security issues. Therefore, it is crucial to account for these combinations, as lower-order threats may combine to create significant security challenges. Additionally, a fully automated, AI-backed system is required for analyzing and implementing security in IoT-based systems.

REFERENCES

[1] Websence Security Lab, *2015 SECURITY PREDICTIONS*, Onliner available at http://www.portantier.com/files/websense-report-2015-security-predictions-en.pdf, 2015.
[2] S. Li, T. Tryfonas and H. Li, *The internet of things: a security point of view*, *Internet Research*, vol. 26, no. 2, pp. 337-359, 2016.
[3] R. Roman, P. Najera and J. Lopez, *Securing the internet of things*, *Computer*, vol. 44, no. 9, pp. 51-58, 2011.
[4] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu and D. Qiu, *Security of the internet of things: perspectives and challenges*, *Wireless Network*, vol. 20, pp. 2481-2501, 2014.
[5] K. Chatterjee, D. Gupta and A. De, *A Framework for Development of Secure Software*, *CSI Transaction on ICT*, vol. 1, no. 2, pp. 143- 157, 2013.
[6] J. Granjal, E. Monteiro and J. S. Silva, *Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues*, *IEEE COMMUNICATION SURVEYS & TUTORIALS*, vol. 17, no. 3, pp. 1294-1312, 2015.
[7] J. A. Stankovic, *Research Directions for the Internet of Things*, *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 3-9, Feburary 2014.
[8] K. Sood, S. Yu and Y. Xiang, *Software Defined Wireless Networking Opportunities and Challenges for Internet of Things: A Review*, *Internet of Things Journal*, vol. 3, no. 4, pp. 453-463, 2015.
[9] B. Martínez-Perez, I. d. l. Torre-Diez and M. Lopez-Coronado, *Privacy and Security in Mobile Health Apps: A Review and Recommendations*, *Journal of Medical Systems*, vol. 39, no. 1, pp. 1-8, 2015.
[10] D. Niewolny, *How the Internet of Things Is Revolutionizing Healthcare, Freescale Semiconductor*, *In Proceedings of International Conference on Healthcare*, pp. 211-219. 2013.
[11] G. Jayavardhana, B. Rajkumar, S. Marusic, and M. Palaniswami, *Internet of Things (IoT): A vision, architectural elements, and future directions*, *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645-1660, 2013.
[12] S. Lee, G. Tewolde, and J. Kwon, *Design and Implementation of Vehicle Tracking System Using GPS/GSM/GPRS Technology and Smartphone Application*, In *IEEE World Forum on Internet of Things (WF-IoT), Seoul, 2014*, pp. 353-358, 2014.
[13] D. Barnard-Wills, L. Marinos, and S. Portesi, *Threat Landscape and Good Practice Guide for Smart Home and Converged Media*, *ENISA (The European Network and Information Security Agency)*, pp. 175, 2014.
[14] A. Mitrokotsa, M. Beye, and P. Peris-Lopez, *Classification of RFID Threats based on Security Principles*, *Security Lab, Faculty of Electrical Engineering, Mathematics and Computer Science, Delft University of Technology*, 2011.
[15] CRAMM, *United Kingdom Central Computer and Telecommunication Agency (CCTA)*, emphRisk analysis and management method, CRAMM user guide, Issue 5.1., 2005.

[16] F. d. Braberl, I. Hogganvik, M. Lund, K. Stølen, and F. Vraalsen, *Model-based security analysis in seven steps—a guided tour to the CORAS method*, *BT Technology Journal*, vol. 25, no. 1, p. 101–117, 2007.
[17] B. A. Forouzan, *Cryptography & Network Security*, *The MsGraw Hill Companies*, pp. 721, 2008.
[18] B. Chamberlin, *IBM Center for Applied Insights*, Available at: https://ibmcai.com/2016/03/01/healthcare-internet-of-things-18-trends-to-watch-in-2016/., 2016.
[19] Wikipedia, *Available at: http://www.wikipedia.com Accessed January 2016*.
[20] Gartner, *21 Billion IoT Devices To Invade By 2020*, Available: http://www.informationweek.com/mobile/mobile-devices/gartner-21-billion-iot-devices-to-invade-by-2020/d/d-id/1323081. 2020.
[21] IDC, *Explosive Internet of Things Spending to Reach $1.7 Trillion in 2020*, Available at: http://www.idc.com/getdoc.jsp?containerId=prUS25658015, 2020.
[22] L. O'Donnell, *IOT Predictions for 2016*, Available at: http://www.crn.com/slide-shows/networking/300079629/10-iot-predictions-for-2016.htm?itc=refresh, 2016.
[23] OWASP, *OWASP Risk Rating Methodology*, Available at: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology, 2014.
[24] M. Hossain, R. Hasan, A. Skjellum, *Securing the Internet of Things: A Meta-Study of Challenges, Approaches, and Open Problems In Proceedings of the 2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW), Atlanta, GA*, pp. 220–225, 2017.
[25] K. Park, D. H. Shin, *Security assessment framework for IoT service Telecommun. Syst.*, vol. 64, pp. 193–209, 2017.
[26] P. Schaumont, *Security in the Internet of Things: A challenge of scale*, In *Proceedings of the Design, Automation & Test in Europe Conference & Exhibition (DATE), Lausanne, Switzerland*, pp. 674–679, 2017.
[27] S. Jaiswal, D. Gupta, *Security Requirements for Internet of Things (IoT)*, In *Proceedings of International Conference on Communication and Networks, Advances in Intelligent Systems and Computing*, Springer: Singapore, Vol. 508, pp. 419–427, 2017.
[28] R. Tourani, S. Misra, T. Mick, G. Panwar, *Security, Privacy, and Access Control in Information-Centric Networking: A Survey*, *IEEE Commun. Surv. Tutor.* vol. 20, pp. 566–600, 2017.
[29] W. Zhou, Y. Zhang, P. Liu, *The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved*, *IEEE Internet Things J.* vol. 6, 2018.
[30] M. Ammar,G. Russello, B. Crispo, *Internet of Things: A survey on the security of IoT frameworks*, *J. Inf. Secur. Appl.*, vol. 38, pp. 8–27, 2018.
[31] S. Asiri, *A Blockchain-Based IoT Trsust Model, Master's Thesis, Ryerson University, Toronto, ON, Canada*, 2018.
[32] A. V. Jerald, S. A. Rabara, D. P. Bai, *Secure IoT architecture for integrated smart services environment*, In *Proceedings of the 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), Palladam, India*, pp. 800–805, 2016.
[33] A. Sedrati, A. Mezrioui, *Internet of Things challenges: A focus on security aspects*, In *Proceedings of the 8th International Conference on Information and Communication Systems (ICICS), Jeju, Korea*, pp. 210–215, 2017.
[34] A. Oracevic, S. Dilek, S. Ozdemir, *Security in Internet of Things: A survey*, In *Proceedings of the 2017 International Symposium on Networks, Computers and Communications (ISNCC), Marrakech, Morocco*, pp. 1–6, 2017.
[35] A. Dey, S. Nandi, M. Sarkar, *Security Measures in IoT based 5G Networks*, In*3rd International Conference on Inventive Computation Technologies (ICICT 2018), Coimbatore, India*, pp. 561-566, 2018 doi: 10.1109/ICICT43934.2018.9034365.
[36] M. Gupta, V. P. Singh, K. K. Gupta, P. K. Shukla, *An efficient image encryption technique based on two-level security for internet of things*, *Multimedia Tools and Applications*, vol. 82, pp. 5091–5111, 2022, doi: 10.1007/s11042-022-12169-8.
[37] N. S. Khan, M. A. Chishti, *Security Challenges in Fog and IoT, Blockchain Technology and Cell Tree Solutions: A Review*, *Scalable Computing: Practice and Experience*, vol. 21, no. 3, pp. 515–542, 2020, doi: 10.12694/scpe.v21i3.1782.
[38] S. Pal, M. Hitchens, T. Rabehaja, S. Mukhopadhyay, *Security Requirements for the Internet of Things: A Systematic Approach*, *Sensors* vol. 20, no. 1 pp. 5897, 2020, doi: https://doi.org/10.3390/s20205897
[39] H. Bansal, S. Jaiswal, *Lay a hand on IOT with SAP Leonardo in Data Acquisition and Processing*, vol. 38 no. 1, pp. 5374-5392, 2023.
[40] H. Sharma, P. Kumar, K. Sharma, *Recurrent Neural Network based Incremental model for Intrusion Detection System in IoT*, *Scalable Computing: Practice and Experience*, vol. 25, no. 5, pp. 3778-3795, 2024.

Edited by: Manish Gupta
Special issue on: Recent Advancements in Machine Intelligence and Smart Systems
Received: Sep 13, 2024
Accepted: Nov 27, 2024