CHAPTER 2

LITERATURE SURVEY

2.1 INTRODUCTION

This chapter describes the literature review linked to this research field. It includes the techniques for real time data collection, processing storage techniques using IoT, layered architecture of IoT, security issues and applications of IoT. A broad range of cryptographic algorithms have been developed to ensure secure transmission of information through the internet. These cryptographic algorithms are employed as conventional algorithms have limitations in low power resource constrained devices. The chapter also discusses about lightweight cryptographic algorithms in embedded or low powered devices. An overview of SCM and cold chain networks is described. Cold chain management for perishable goods in a limited-scale setting indeed comes with its own set of unique challenges and considerations. The essential requirements and challenges of SCM for small-scale cold chain applications are discussed.

2.2 INTERNET OF THINGS

The IoT refers to a network of interconnected physical devices, vehicles, appliances, and other objects embedded with sensors, software, and connectivity capabilities. These devices can collect and exchange data over the internet, enabling them to interact with their environment and communicate with each other. IoT is also an Internet Technology connecting devices, machines and tools to the Internet using wireless technologies like Bluetooth, WiFi, Zigbee. IoT results in the unification of technologies such as low power embedded systems, cloud computing, big data, machine learning and networking. The two solutions for the networking technologies are either to expand the existing network or to build a separate system from scratch. (Hassan et al., 2019).

The concept of IoT revolves around the idea of connecting everyday objects to the internet, allowing them to be remotely monitored, controlled, and managed. This connectivity opens a wide range of possibilities and applications across various domains,

including smart homes, smart cities, industrial automation, healthcare, agriculture, transportation, and more.

The below sections give an overview of the components of IoT and the layered architecture of IoT. Then, it describes the applications in the areas of IoT. It also discusses the general security issues and current available IoT solutions.

2.2.1. Components of IoT

IoT works on four different components as shown in Figure 2.1 (Kumar et al., 2018):

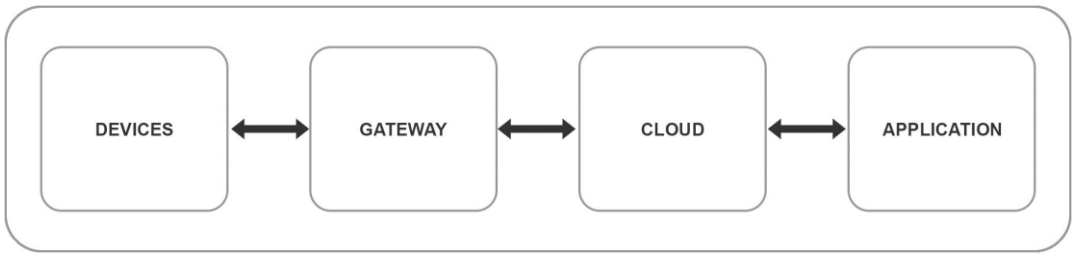

Figure 2.1 IoT Components

- **Devices:** These are the physical objects or "things" that are equipped with sensors, actuators, interfaces, microcontrollers and connectivity capabilities. Examples include smartphones, wearable devices, smart home appliances, industrial sensors, and autonomous vehicles.

- **IoT Gateways**: Gateways acts as an intermediate node to collect data from the end devices and transmit it to the internet. IoT devices rely on various communication technologies to connect to the internet and exchange data. This includes Wi-Fi, Bluetooth, cellular networks, Zigbee, Radio Frequency Identification (RFID) and others.

- **Data Processing and Analytics:** The massive amounts of data generated by IoT devices require processing and analysis to derive meaningful insights. Cloud platforms and edge computing technologies are used to store, process and analyze IoT data, enabling real-time decision-making and intelligent automation. The data collected by the sensors have to be stored and processed intelligently within the cloud infrastructure.

- **Applications:** IoT technology enables a wide range of applications across industries. Some examples include smart homes with connected appliances, energy management systems, remote patient monitoring in healthcare, predictive maintenance in manufacturing and traffic management in smart cities. Applications will support the end users to control and monitor the smart devices from remote locations.

These components work together to enable the collection, communication, processing, and analysis of data in IoT systems. Sensors/devices collect data, connectivity facilitates data exchange, data processing enables insights, cloud services provide storage and computing capabilities and applications allow users to interact with IoT devices.

The IoT components can be broadly categorized into six key aspects, each serving a crucial role in the functioning and effectiveness of an IoT system.

The key aspects of IoT components are:

- Identify

The "Identify" component refers to the unique identification and addressing of IoT devices and objects within the network. Each IoT device or sensor is assigned a specific identifier or address that enables its recognition and differentiation from other devices. Identifiers may be in the form of unique device IDs, Media Access Control (MAC) addresses, Internet Protocol addresses or other unique codes.

- Sense

The "Sense" component involves the use of various sensors and actuators to capture data from the physical environment. Sensors collect information such as temperature, humidity, pressure, light, motion, sound and more, depending on the specific application. Actuators, on the other hand, enable IoT devices to interact with the environment by performing actions based on the collected data.

- Communicate

The "Communicate" component enables data transmission and exchange between IoT devices, sensors, and the central data processing units. This involves using various

communication protocols and technologies such as Wi-Fi, Bluetooth, Zigbee, RFID, cellular networks, or Low Power Wide Area Network. Effective communication is vital for seamless data transfer and real-time interaction in IoT systems.

- Compute

The "Compute" component involves data processing and analysis. Once the data is collected from sensors, it needs to be processed, aggregated, and analyzed to derive meaningful insights and actionable information. This can occur in various locations, such as on the edge computing or in the cloud computing depending on the specific use case and requirements.

- Services

The "Services" component encompasses the various applications and functionalities that leverage the processed data to provide value to users. IoT services can include applications for home automation, smart city solutions, industrial monitoring, healthcare, environmental monitoring, and more. These services utilize the data to deliver specific benefits and enhance user experiences.

- Semantics

The "Semantics" component involves adding meaning and context to the collected data. It allows for the standardization and interpretation of data from different sources. By defining a common language and structure for data representation, semantics ensure that various devices and systems can understand and interpret data uniformly regardless of their origin.

Overall, these six components work together to create a comprehensive IoT ecosystem where data is efficiently collected, communicated, processed, and transformed into actionable insights, providing valuable services and experiences to users and enabling the realization of the full potential of the IoT.

2.2.2. Layered Architecture of IoT

The key components of IoT consists of devices, gateways, cloud and application. The layered architecture of the IoT (Grønbæk, I.et al., 2008, Wu, M.et al., 2010) refers to an abstraction or conceptual framework that organizes the components and functionalities of IoT systems into distinct layers. This architecture helps in understanding, designing, and implementing IoT systems in a modular and scalable manner. In the Layered view the system is viewed as a complex heterogeneous entity that can be decomposed into interacting parts.

The IoT supports billions of objects, has a greater need of big data storage and more communication traffic. The Transmission Control Protocol/Internet Protocol used for network communication fails to meet these demands of IoT. The architecture proposed for IoT must meet the requirements of scalability, reliability, Quality of Service, interoperability etc. The layered architecture of IoT is designed to address the complex and multifaceted nature of IoT systems. Its characteristics promote flexibility, scalability, Quality of Service, security, and interoperability while allowing for efficient management of resources and data. This makes it a robust framework for building and deploying IoT solutions in a wide range of industries and applications.

Various layered architecture has been proposed (Al-Qaseemi et al., 2016, Ahemd, M. M., et al., 2017, S. A., Sethi, P., & Sarangi, S. R., 2017) and they differ in layers like three, four, five. The layered architecture serves specific purposes, and there are both benefits and limitations associated with this architecture. Additionally, there are various platforms (S.Soursos et al., 2016) protocols (Ponnusamy, K., & Rajagopalan, N.,2018) and applications(Zeinab,K.A.M.,et al., 2017) that align with this architecture. Typically, the architecture's division into three layers promotes modularity and scalability, interoperability, simplified development, flexibility, and ease of maintenance. The additional middleware layer in the four layered architecture facilitates data filtering, aggregation, protocol translation, security and device management. The concept of a five-layered architecture in the context of the IoT may not be as

standardized as the three or four-layered architectures. The inclusion of the business layer focuses on business logic, analytics and decision-making based on the processed data, leading to informed actions. There are several development platforms that align with the three-layered architecture of IoT, such as Arduino, Raspberry Pi and Node-RED. The Edge computing platforms, middleware solutions are the commonly used platforms in four-layer architecture. Some of the platforms (Paudel, N., & Neupane, R. C.,2019) used for business layer in five layered architecture are Tableau, Microsoft Power BI, ThingWorx.IoT Protocols involve Message Queuing Telemetry Transport (MQTT), Constrained Application Protocol which is designed for resource-constrained devices, and suitable for the Network Layer in IoT environments. Hypertext Transfer Protocol (HTTP) which is commonly used in the Application Layer for communication between IoT applications and end-users. Additional IoT Protocols used in four-layer architecture are Advanced Message Queuing Protocol. Custom Application Programming Interface (API), Representational State Transfer, Open Data Protocol are needed to integrate the business layer. The limitations (Al-Qaseemi, S. A., et al., 2016) of three-layer architecture are complex integration, data overhead, latency, security challenges and overhead in resource-constrained devices. Integration complexity, potential latency, security challenges are some of the limitations of four-layer architecture. Integration of IoT data into existing business processes and addressing privacy concerns can be complex in five layered architecture. The major applications of middleware layer in four layered architecture consists of data processing, protocol translation, device management, security enforcement. Data aggregation, local analytics, event-driven actions are some of the applications areas of business layer in five layered architecture.

The Three-layer architecture is the basic layered architecture for IoT as shown in Figure 2.2. The three-layered architecture of IoT (Sha.K, et al., 2018) simplifies the complexities of IoT systems by dividing them into three distinct layers: the Perception Layer, the Network Layer and the Application Layer.

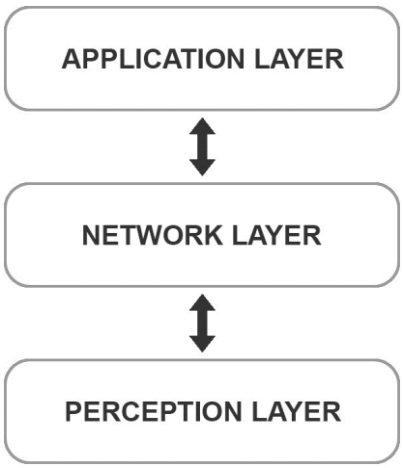

Figure 2.2 Three-layered architecture of IoT

The different layers in three-layer architecture of IoT consists of:

- **Perception layer:** Aforementioned is the physical layer for sensing and collecting information from the environment. It comprises the physical devices, sensors, actuators, and embedded systems that interact with the physical world. These devices capture data from the environment or control physical objects based on received instructions. Examples include temperature sensors, motion detectors, cameras, and actuators like motors or valves.

- **Network layer:** This layer transfers the sensor data from the perception layer to the next layer and vice versa through the networks. The network layer focuses on the communication infrastructure and protocols used to connect the IoT devices and enable data transfer. This layer encompasses both Local Area Network (LAN) and Wide Area Network (WAN). It includes technologies such as Wi-Fi, Bluetooth, Zigbee, RFID, cellular networks, and satellite communications. The network layer ensures reliable and secure transmission of data between devices and other layers of the IoT architecture.

- **Application layer:** This layer is responsible for delivering application-specific services to the user. It defines various applications that can be deployed using IoT. The application layer is the topmost layer of the IoT architecture and represents the user-

facing part of the system. It encompasses the applications, services and interfaces that leverage the data collected from IoT devices to provide value-added functionality and enable specific use cases.

The three-layered architecture provides a simplified framework, real-world IoT systems can be more complex and may involve variations or combinations of these layers to suit specific needs. While the common three-layered architecture is widely recognized, variations exist that may add more layers to address specific requirements.

The architecture of an IoT system can be broken down into four layers with the addition of middleware layer, each serving a specific purpose in the data flow and communication process as shown in Figure 2.3.

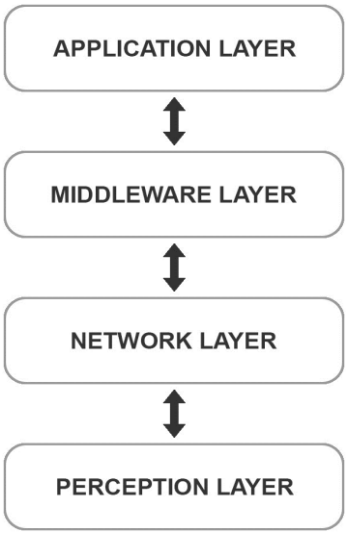

Figure 2.3 Four-layered architecture of IoT

Middleware layer is responsible for receiving data from the network layer to process and store system data in the cloud and database. It also feeds the application layer with the required APIs. The storage and computational capacity of the middleware layer is a function of advanced cloud computing and IoT development. Service quality in the application layer is also determined by the security of the cloud and database (Alaba, F. A, et al., 2018)

The five-layered architecture of IoT as in Figure 2.4. typically includes the addition of topmost business layer.

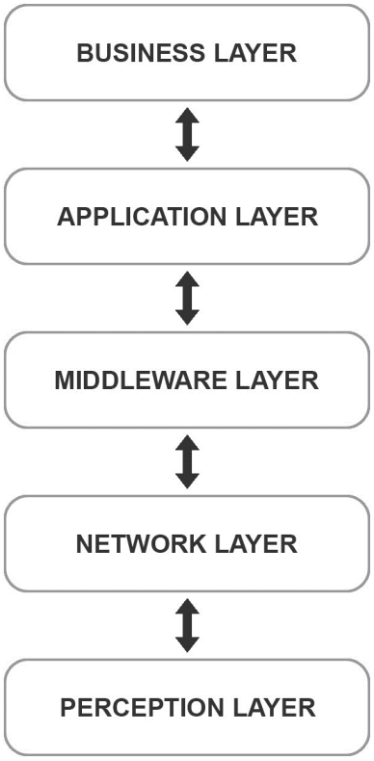

Figure 2.4 Five-layered architecture of IoT

The business layer is the topmost layer of the IoT architecture. It focuses on the integration of IoT technologies into the overall business processes and strategies. This layer involves business-specific applications and services that leverage IoT data to drive organizational growth, efficiency, and innovation. It may include business intelligence tools, data analytics platforms, and other solutions that help businesses make informed decisions based on the IoT-generated data.

In summary, the five-layered architecture of IoT, consisting of the Perception, Network, Middleware, Application, and Business layers, forms a comprehensive framework for designing, deploying, and managing IoT systems. Each layer plays a vital role in the data flow, processing and utilization to enable the seamless integration of

physical devices and the digital world, ultimately creating valuable and impactful applications and services.

In the six and seven-layered architectures, the added layers such as Data Management and Analytics layers provide a more granular view of the data processing and analysis stages in the IoT system. This can be beneficial in scenarios where there is a strong emphasis on advanced data analytics and intelligence for decision-making or when a more detailed breakdown of the data flow and processing is required.

It's important to note that the number of layers and the specific names of each layer can vary depending on the context and the requirements of an IoT implementation. The essential components remain the same across different architectures: data collection, communication, data processing, application development, security and business integration.

Security is a critical concern in IoT systems, especially between the perception layer and the network layer, as this is the point where data from physical devices starts to transition into the digital realm. Implementing robust security measures at this juncture is essential to protect both the devices and the data being transmitted. Encryption of data is required which could protects the confidentiality of data in transit, preventing unauthorized parties from intercepting and understanding the data. The use of cryptographic algorithms to encrypt data as it is transmitted over the network for resource constrained devices is necessary to maintain the security of IoT systems from the perception layer to the network layer and beyond.

2.2.3. Applications of IoT

Currently IoT systems are used in logistics sector where the application has been used to track the items placed in racks in the supermarket. In the shopping mall people are connected through IoT to know about the new offers of a product in different shops (Pathan, A et al., 2016). Applications such as customer tracking and analysis, dynamic pricing has been identified by incorporating IoT with data mining techniques

(Đurđević,N et al., 2017). A mathematical model (Mani, Z et al., 2017) has been proposed in conjunction with IoT to find out the best pattern from several categories for e-commerce applications. Internet of things has been used as an instrument for marketing in the digital marketing sector. IoT has created an impact on warehouse and yard management (Tadejko, P. et al., 2015), shrinkage and misplacement of inventory (Fan, T.et al., 2015) and accurate and timely delivery of products using sensor enabled RFID networks. By taking autonomous decisions using sensor networks (Ben-Daya, M.et al., 2019) positive benefits has been received by the manufacturer, distributor and customers.

The IoT has a wide range of applications (Yao, J.,2017) across various industries. Some common applications of IoT include Smart Home automation, Industrial Automation, Agriculture, Healthcare, Smart Cities, Energy Management, Retail, Transportation and Logistics, Environmental Monitoring and Wearable Devices.

2.2.4. Security threats and solutions in IoT

The IoT has the challenges related to security, privacy, scalability, and data management even though it has the potential to transform industries, improve efficiency, enhance quality of life and create new opportunities. IoT security is a critical aspect due to the potential vulnerabilities associated with connected devices. Ensuring the confidentiality, integrity and availability of data, as well as protecting against unauthorized access and cyber-attacks, is of utmost importance. Privacy concerns (Chaurasia, N.et al., 2023) related to the collection and use of personal data by IoT devices also need to be addressed.

Interoperability and standardization are essential for seamless integration and communication between different IoT devices and systems. Standardization organizations like the Internet Engineering Task Force (IETF), the International Organization for Standardization (ISO), and the Institute of Electrical and Electronics Engineers (IEEE) work on developing and maintaining IoT standards and protocols.

Each layer has its security (Song, T.,et al., 2017), (Tewari, A.,et al., 2020) concerns. In the basic three-layered architecture, several security issues fall in the perception, network and application layer. Node Capture, Fake Node and Malicious Data, Denial of Service Attack, Replay Attack are some of the frequent attacks of the perception layer. Attacks like eavesdropping, man in the middle, Denial of Service, Network Intrusion are common threats at the network layer. Some of the security and privacy issues at the application layer are Mutual Authentication and Node Identification, Information Privacy, Data Management and Application Specific Vulnerabilities.

There are several mechanisms to protect IoT applications in the layered architecture (Burhan et al., 2018). In the perception layer we have Hash based encryption, Public Key Infrastructure (PKI), Secure Authorization, Lightweight Cryptography and Embedded Security Framework. In the network layer we have Identity management framework, Risk based adaptive system, Software Defined Networking with IoT, Cooperation of Nodes Communication Protocol, Reputation System based mechanism and Cluster based Intrusion Detection System. Preference based protection, Access control mechanism, OpenHab Technology, IoTOne Technology, and Identity based framework are some of the mechanisms to protect IoT applications in the application layer.

Hash based encryption (Li, F.et al., 2013,Sundaram,B.V.et al., 2015) is a type of lightweight cryptography that utilizes cryptographic hash functions for encryption purposes. It is often used in scenarios where traditional encryption algorithms may be too resource-intensive for resource-constrained devices, such as those found in IoT and other embedded systems. The main idea behind hash-based encryption is to leverage the properties of cryptographic hash functions to achieve confidentiality and integrity for the transmitted data. Hash-based encryption typically provides confidentiality and integrity without requiring complex arithmetic operations, making it suitable for resource-limited environments. However, it is essential to choose a secure cryptographic hash function and a robust key derivation function to ensure the security of the overall scheme.

For lightweight cryptography scenarios, traditional PKI protocols may be too resource-intensive due to the computational overhead associated with public key operations. Therefore, several lightweight variants of PKI-like protocols have been developed to suit the constraints of resource-constrained devices. These lightweight alternatives often focus on simplicity, efficiency and reduced computational requirements. One such example is the "Hash-Based Public Key Infrastructure" (Weber, R. H, et al., 2010 Li, Z. et al., 2013), which combines hash functions and digital signatures to achieve a lightweight PKI like protocol. One of the advantages of Hash-Based Public Key Infrastructure is lightweight nature, as it relies on the efficiency of hash functions for key validation rather than computationally-intensive public key operations like modular exponentiation. However, it is important to note that hash-based cryptography may be susceptible to certain types of attacks, and the security of Hash-Based Public Key Infrastructure depends on the chosen hash function's resistance to collision and preimage attacks.

Securing the authorization mechanism with OAuth (Cirani, S.et al., 2013) in the perception layer of IoT applications is crucial for ensuring that only authorized devices and applications can access and interact with sensory data. The perception layer comprises sensors, actuators and edge devices that collect and process data from the physical environment. Secure communication, OAuth Token Usage, Token validation and revocation, Device authentication are some of the secure authorization mechanisms with OAuth in the perception layer.

Embedded security frameworks (Ravi, S. et al., 2004, Babar, S. et al., 2011) provide a structured approach for implementing security measures in resource-constrained IoT devices. The essential components of an embedded security framework for the perception layer of IoT applications are Secure Boot, Hardware-Based Security, Secure Communication, Secure Firmware Updates, Security Testing and Certification, Continuous Monitoring and Auditing. By integrating these security measures into the embedded systems within the perception layer, IoT applications can significantly enhance their overall security and reduce the risk of potential vulnerabilities and attacks.

In the network layer of IoT devices, identity management (Horrow, S., & Sardana, A.,2012) is critical for ensuring secure communication, access control, and authentication among the devices and network components. An identity management framework in the network layer of IoT devices encompasses various components and functionalities to handle identity-related tasks. By incorporating identity management practices like Unique Device Identifiers, Device Authentication, Secure Communication Protocols, Secure Boot and Firmware Validation into the network layer of IoT devices, organizations can establish a robust and secure infrastructure, ensuring that only authorized and authenticated devices participate in the IoT ecosystem while minimizing security risks.

A risk-based adaptive system (Abie, H.et al., 2012) in the network layer for IoT devices is designed to dynamically adjust network security measures and access controls based on the perceived risk associated with each device and its behaviour. This approach helps to enhance the overall security of the IoT network while minimizing the impact on legitimate operations. By incorporating risk-based adaptation into the network layer security framework for IoT devices, organizations can adopt a more proactive approach to network security.

Software Defined Networking (Robertazzi, T.G.& Robertazzi, T.G.,2017), (Al Shuhaimi, F.et al., 2016) allows for the centralization of network control and enables programmability and automation, which align with the dynamic nature of IoT environments. By integrating Software Defined Networking with IoT in the network layer, organizations can build flexible and scalable network infrastructures that can efficiently support the diverse requirements of IoT devices and applications.

In the network layer of IoT devices, the cooperation of nodes communication protocol (Buchegger, S. & Le Boudec, J. Y.,2002) plays a crucial role in facilitating efficient and reliable communication among IoT devices. This protocol enables IoT devices to cooperate with each other, exchange data and work collaboratively to achieve specific tasks or objectives. The cooperation of nodes communication protocol ensures

that IoT devices can interact seamlessly, optimize network resources and collectively solve complex problems. Cooperation of nodes communication protocol in the network layer enables IoT devices to work synergistically, effectively leveraging the collective capabilities of the network. By fostering collaboration and data exchange among IoT devices, the protocol enhances the overall performance, scalability, and adaptability of the IoT ecosystem.

A Reputation System-based mechanism (Michiardi, P. &Molva, R.,2002) and a Cluster-based Intrusion Detection System (IDS) (Oke, J. T. et al., 2018) are two effective approaches for enhancing security in the network layer of IoT systems. A Reputation System is a mechanism that assesses the trustworthiness and reliability of individual IoT devices based on their past behaviour and interactions within the network. In the network layer of IoT systems, a Reputation System can help identify and isolate potentially malicious or compromised devices. A Cluster-based IDS is a technique that groups IoT devices into clusters based on similarities in their behaviour and communication patterns. Each cluster operates as a cohesive unit and the IDS detects anomalies or intrusion attempts by monitoring the behaviour of devices within these clusters. By combining a Reputation System-based mechanism and a Cluster-based IDS, the network layer of IoT systems can achieve a more robust and proactive security posture.

Preference-based protection (Wenjun, L.,2010, Yang, Z.,2010 & Tao, H. et al., 2010) in the application layer of IoT devices involves allowing users to customize and set their security preferences based on their individual requirements and risk tolerance. This approach empowers users to make informed decisions about the security measures applied to their IoT devices and data, striking a balance between security and usability. By incorporating preference-based protection in the application layer of IoT devices, manufacturers and developers can empower users to take an active role in securing their IoT ecosystem.

Access control mechanisms (Bormann, C. et al., 2012, Gupta, K. et al., 2016) in the application layer of IoT devices are crucial for ensuring that only authorized users or

applications can interact with the device's functionalities and sensitive data. These mechanisms help to protect the device from unauthorized access, data breaches and potential security threats. The selection of the appropriate access control mechanism(s) depends on the specific IoT application, the level of security required and the user's preferences.

OpenHAB (Gyory, N.et al., 2017) is an open-source technology designed for the application layer of IoT devices. It is a vendor and technology-agnostic home automation platform that enables users to connect, control, and automate a wide range of IoT devices and services from various manufacturers. OpenHAB provides a unified and customizable interface for managing smart home devices, making it a popular choice for IoT enthusiasts and home automation enthusiasts. OpenHAB's flexibility, versatility and strong community support make it an attractive choice for home automation enthusiasts and professional IoT projects. Its ability to integrate with a wide range of devices and technologies allows users to create a unified and centralized smart home ecosystem, providing a seamless user experience for managing IoT devices in the application layer.

An identity-based security framework (Sarma,A.et al., 2008,Hu,C.et al., 2011) in the application layer for IoT devices focus on ensuring secure and authenticated access to IoT applications and services based on the identities of users, devices, entities involved in the communication. This framework plays a crucial role in safeguarding sensitive data, controlling access to IoT resources and preventing unauthorized actions within the IoT ecosystem. An identity-based security framework for IoT devices in the application layer provides a solid foundation for protecting sensitive data, ensuring secure access control and mitigating potential security risks within the IoT ecosystem.

Unified identity authentication, session security, malicious code detection (Zhang, W., et al., 2013) are some of the solutions to protect applications in the middleware layer. Policy based firewalls, advanced encryption mechanisms are some of the security solutions in the business layer. (Pahlevanzadeh, B.,2020).

Selective forwarding, synchronization attacks, replay attack, denial of service, man-in-the-middle attacks, SQL injection are possible on IoT environment. (Hassija, V,et al., 2019) suggested the security risks, enhancements and solution architectures that IoT applications need. The work outlines the protection and privacy problems concerning various IoT applications. Blockchain, Fog computing, Machine learning and edge computing based solutions are proposed for securing IoT environments and applications. (Burhan, M.et al., 2018) suggested a modern and standardized six-layer protected architecture for IoT. The paper addressed the use of communication technologies in IoT applications. (Hammi M et al., 2017) created a robust, fast and lightweight symmetric encryption algorithm for IoT devices. (Arsalan Mosenia et al., 2016) outlined weaknesses that IoT's edge side layer. (Y.yang et al., 2017) addressed the drawbacks of IoT devices. (L.chen et al., 2017) focuses on location-specific security issues in IoT . (Ngu, A.H et al., 2016) addressed IoT middleware-related security problems. To enhance security in Internet of Things (IoT) systems, various solutions and best practices (Rizvi, S et al., 2018) can be implemented.

With the increasing reliance on digital systems and interconnected networks, data breaches have become a significant concern. Cryptography is the process of encryption and decryption of data thereby removes the major challenges in IoT network. Cryptography is a fundamental component of securing data and communications. It involves the use of mathematical algorithms and techniques to transform plaintext (original data) into ciphertext (encrypted data) and vice versa. There are several types of cryptography (Gan, A. et al., 2021) each serving different purposes and offering varying levels of security (Sharma, S., & Gupta, Y., 2017) as shown in Figure 2.5.

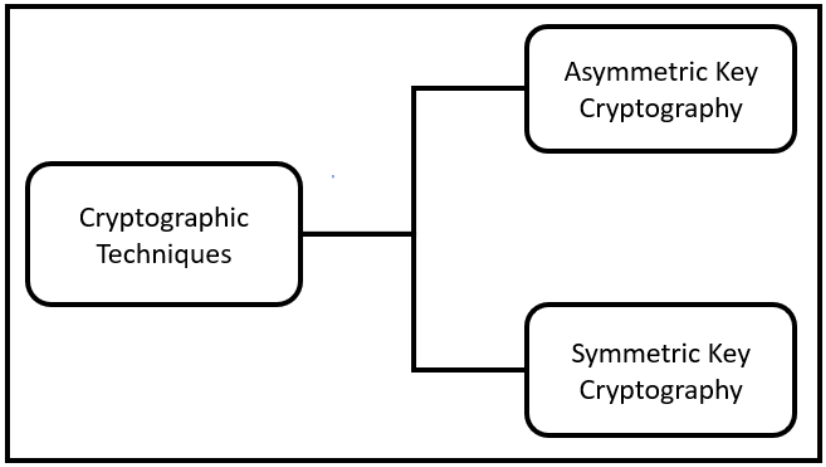

Figure 2.5 Types of cryptography techniques

Symmetric Key Cryptography: Also known as secret-key or shared-key cryptography, symmetric key cryptography uses a single key for both encryption and decryption (Mewada, Sharma, & Gautam, 2016). The same key is used by both the sender and the receiver to encrypt and decrypt the data. Examples of symmetric key algorithms include Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Triple DES.

Asymmetric Key Cryptography: Asymmetric key cryptography, also called public-key cryptography, uses a pair of mathematically related keys: a public key and a private key. The public key is freely distributed and used for encryption, while the private key is kept secret and used for decryption. Asymmetric key cryptography provides a mechanism for secure key exchange and digital signatures. Common asymmetric key algorithms (Abood & Guirguis, 2018) include Rivest-Shamir-Adleman, Diffie-Hellman, and Elliptic Curve Cryptography.

Cryptography offers several benefits when it comes to securing data and communications, but it also has certain limitations. The benefits of cryptography (Mitali et al.; Sharma et al., 2014) are Confidentiality, Data Integrity, Authentication, Non-repudiation, Secure Key Exchange, Compliance and Regulations, Secure

Communication, Key Management, Public Key Infrastructure, Privacy Protection. Cryptography ensures the confidentiality of data by encrypting it. Encrypted data is unreadable to unauthorized parties, providing a strong layer of protection against data breaches and unauthorized access. Cryptographic techniques, such as hash functions and digital signatures, enable verification of data integrity. Any unauthorized changes to the data can be detected through hash value mismatches or signature verification failures, ensuring the data's integrity. Cryptography allows for the verification of the identity of communicating parties. Digital certificates, digital signatures and PKI enable authentication of sender and receiver. Digital signatures provide non-repudiation, meaning the signer cannot deny their involvement in signing a document. This is crucial for legal and business transactions where proof of authenticity and accountability is required. Cryptography provides methods for secure key exchange between parties. Protocol like Diffie-Hellman allow two parties to agree on a shared secret key over an insecure channel without exposing the key to eavesdroppers. Cryptography helps organizations comply with various regulatory requirements for data protection and privacy, such as the General Data Protection Regulation or the Payment Card Industry Data Security Standard. It facilitates secure communication channels, protecting data during transmission over potentially insecure networks, like the internet. It also includes methods for secure key exchange and management, ensuring that encryption keys are shared and stored securely. Cryptography supports PKI, a system that enables secure authentication and encryption using public and private key pairs. Cryptography helps to protect the privacy of individuals, ensuring that personal data remains confidential.

The limitations of cryptography are Key management, Computational Overhead, Key Exchange and Trust, Vulnerabilities, Side-Channel Attacks, Human Factors, Performance Impact, Human Error, Backdoors and Misuse, Quantum Computing Threat, Cost and Complexity. Cryptography requires effective key management practices. The secure generation, distribution, storage and revocation of keys can be complex and resource-intensive, especially in large-scale systems. Strong cryptographic algorithms often involve complex mathematical computations, which can introduce computational

overhead. Encryption and decryption processes may slow down system performance, particularly when dealing with large volumes of data. Cryptography relies on secure key exchange and establishing trust between communicating parties. If the initial key exchange is compromised or if there are issues with trust, the security of the cryptographic system can be compromised. It can be vulnerable to attacks if implemented incorrectly or if there are weaknesses in the algorithms or protocols used. Cryptanalysis techniques, such as brute force attacks or vulnerabilities in specific algorithms, can potentially undermine the security of encrypted data. Cryptographic implementations can be susceptible to side-channel attacks that exploit information leaked during the encryption or decryption process. These attacks include timing analysis, power analysis, or electromagnetic radiation analysis. Cryptography relies on human actions, such as proper key handling, passphrase selection, and secure system configurations. Human errors, such as weak passwords or misconfigurations, can undermine the effectiveness of cryptographic controls. Strong encryption algorithms can be computationally intensive, impacting the performance of systems, especially resource-constrained IoT devices. Cryptographic systems can be compromised due to human error, such as poor password management or incorrect implementation. Intentional or accidental misuse of cryptographic tools, such as the inclusion of backdoors by malicious actors, can compromise security. Future advancements in quantum computing may render some current cryptographic algorithms vulnerable to attacks. Implementing and maintaining a robust cryptographic infrastructure can be costly and complex, especially for large-scale systems.

Conventional cryptography (Ahmed, S. et al., 2022) and lightweight cryptography (Thakor,V.A.et al., 2021), are two approaches for securing information and communications, but they differ in terms of their design principles and target applications. Conventional cryptographic algorithms typically use larger key sizes and require significant computational resources, such as processing power and memory. They are often implemented on devices with sufficient resources, such as desktop computers, servers, or high-end mobile devices.

Lightweight cryptography is specifically designed for resource-constrained environments, such as embedded systems, IoT devices, and low-power microcontrollers (O'caoimh, R., et al., 2015). Its primary focus is on providing efficient and lightweight cryptographic solutions with a smaller code size, reduced memory requirement and lower energy consumption. Lightweight cryptography offers efficient and lightweight solutions suitable for resource-constrained devices.

The creation of new cryptographic algorithms that are optimized for IoT devices has been the subject of extensive research over the past decade. These cryptographic methods are frequently referred to as "lightweight" algorithms. Majority of the cryptographic algorithms used today were developed for desktop and server contexts, as a result they are not suitable for small devices. Therefore, lightweight cryptographic approach is proposed that solves many of the problems of traditional cryptography when used on devices with constrained physical size, computational requirements, limited memory and power consumption.

Overall, security solutions are crucial for IoT to protect sensitive data, prevent unauthorized access, ensure the integrity of devices and networks and maintain the trust and confidence of users and stakeholders in the IoT ecosystem. It is important to note that security in IoT is an ongoing effort and should be approached holistically. Applying a combination of these security solutions, along with regular risk assessments can help to mitigate security risks and ensure a safer and more trustworthy IoT environment. Securing real-time data between IoT devices and the platform is crucial in today's era. With the increasing adoption of IoT devices and the vast amount of data generate and transmit, ensuring the security and privacy of the data has become a significant concern.

2.3 LIGHTWEIGHT CRYPTOGRAPHY

Lightweight cryptography refers to cryptographic algorithms and protocols specifically designed for resource-constrained devices, such as low-power microcontrollers, RFID tags, wireless sensors, and smart cards. These devices often have limited processing power, memory, energy and communication capabilities. The goal of

lightweight cryptography is to provide efficient and secure cryptographic solutions that can operate within the constraints of IoT devices. Some key aspects and characteristics of lightweight cryptography are:

- Efficiency: Lightweight cryptographic algorithms are optimized for efficiency, focusing on minimizing computational complexity, memory usage, and energy consumption. These algorithms are designed to perform well on low-power devices with limited resources.
- Security: While lightweight cryptography aims to be efficient, it does not compromise on security. Algorithms designed for lightweight environments undergo rigorous analysis and evaluation to ensure they meet specific security requirements. They typically provide a balance between security and resource constraints.
- Symmetric-key algorithms: Lightweight cryptography often relies on symmetric-key algorithms, such as block ciphers and stream ciphers, for encryption and authentication. These algorithms have a smaller footprint compared to asymmetric (public-key) algorithms, making them more suitable for resource-constrained devices.
- Key size: Lightweight cryptography algorithms often use shorter key sizes compared to traditional cryptographic algorithms. While shorter key sizes may raise concerns about security, the algorithms compensate by employing stronger cryptographic primitives and employing other techniques to mitigate potential attacks.
- Hardware implementation: Lightweight cryptography is often designed with efficient hardware implementations. Hardware accelerators and optimized circuit designs can further improve the efficiency and speed of cryptographic operations on constrained devices.
- Standardization efforts: Several standardization bodies, such as the ISO,IETF and the National Institute of Standards and Technology (NIST), have recognized the need for lightweight cryptography and are actively working on developing standards and guidelines for lightweight cryptographic algorithms.

Lightweight Cryptography (LWC) provides fast and reliable encryption systems for resource constrained devices (Thakor, V.A. et al., 2021). Algorithms designed and implemented according to memory footprint, execution time, security level and resource utilization form a particular set of algorithms called LWC algorithms (Aakash,D et al., 2016). Furthermore, LWC is applicable not only to resource-constrained devices (RFID tags, sensors, etc.) also to resource-rich devices that interacts with servers, PCs, and smartphones. Physical cost and performance traits are met by the LWC algorithm through simplistic round functions on ≤ 64bit using ≤ 80bit key with easy scheduling. The final characteristic security is satisfied by adopting one of the six internal structures for immunity against any security attack. Block ciphers and stream ciphers are two kinds of ciphers wherein the former is a plain text encrypted into a block of bits and the latter is a plain text encrypted into cipher symbol values. Data confidentially relates to encryption of digital data. (Thakor, V.A. et al., 2021). Structurewise classification of LWC Algorithms are shown in Figure 2.6.

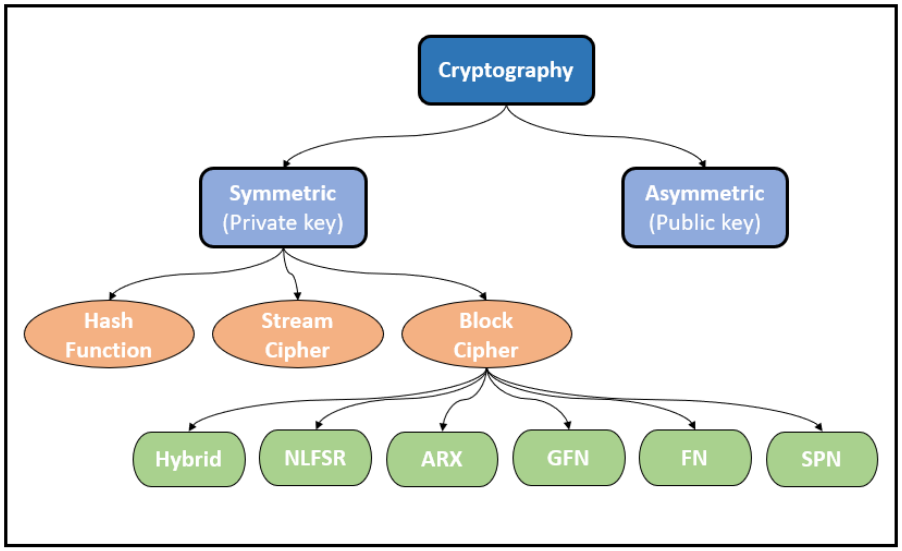

Figure 2.6 Structure wise classification of LWC Algorithms

Real-time use cases for lightweight applications (Thakor, V.A. et al., 2021) with low resource demands are prevalent in various industries, especially in the context of IoT and edge computing. These use cases leverage lightweight technologies and

algorithms to process data quickly and efficiently in resource-constrained environments. Here are some examples of real-time applications with lightweight demands:

- Smart Home Automation: In a smart home, lightweight applications manage real-time tasks such as control lights, temperature, and security systems. These applications run on resource-limited IoT devices and require low-latency response times for immediate user interactions.
- Health and Remote Monitoring: Lightweight healthcare applications enable real-time monitoring of patients' vital signs, activity and health metrics using wearable devices. These applications need to be energy-efficient and low-resource to ensure long battery life for continuous monitoring.
- Asset Tracking and Logistics: Real-time tracking of assets, such as shipping containers, vehicles, or valuable goods, requires lightweight applications that can process location data quickly and transmit updates efficiently over wireless networks.
- Predictive Maintenance: In industry lightweight applications analyse sensor data in real-time to predict and detect equipment failures. These applications optimize maintenance schedules and reduce downtime.
- Environmental Monitoring: Lightweight IoT applications are used for real-time monitoring of environmental parameters such as air quality, water quality and weather conditions. These applications need to be resource-efficient to operate in remote locations and run on battery-powered sensors.
- Gesture Recognition: Real-time gesture recognition in human-computer interaction relies on lightweight algorithms that can process input from cameras or motion sensors quickly and accurately.
- Edge Analytics: Lightweight applications at the edge of the network analyze data locally, reducing the need for transmitting large amounts of data to the cloud. Edge analytics enables real-time insights and faster decision-making.

- Smart Energy Management: In smart grid systems, lightweight applications analyse energy consumption data in real-time, enabling automated load balancing and demand response mechanisms.
- Traffic Management: Lightweight applications process real-time data from traffic sensors and cameras to optimize traffic flow, reduce congestion and improve road safety.
- Smart Agriculture: Real-time applications in agriculture use lightweight technologies to monitor soil conditions, crop health, irrigation systems, improving resource efficiency and crop yields.
- Consumer Wearables: Lightweight applications on wearable devices, such as fitness trackers and smartwatches, provide real-time health and fitness monitoring without draining the device's battery quickly.

In these real-time use cases, lightweight demands are critical to ensure efficient use of resources, extended battery life, and fast response times. Lightweight applications are designed to strike a balance between functionality and resource efficiency, making them ideal for deployment in resource-constrained environments, such as IoT devices, edge nodes, and other low-power embedded systems.

2.3.1. Lightweight Encryption and Decryption algorithms

Cryptosystems can be classified into symmetric and asymmetric cryptosystems. Symmetric cryptography is further classified into 2 types - Block cipher and Stream cipher. Symmetric block ciphers are easy to implement due to its operations like substitution, permutation, key addition, mixing which provide strength to algorithm (Razaq, A. et al., 2021). Block ciphers are further divided into six internal structures and among that substitution permutation network can tweak data through substitution box and permutation table. AES is (Chom Thungon, L et al., 2018) a widely accepted symmetric encryption algorithm. Since it requires large memory space and high power for computation it is not desirable for resource constrained devices.

LWC algorithms are designed to be resource-efficient and suitable for use in constrained environments like IoT devices and other low-power systems. Standardization ensures interoperability, security and widespread adoption of these algorithms across different platforms and applications. Several organizations and initiatives have been working on standardizing LWC algorithms. Here are some key developments:

- NIST LWC Competition: NIST launched a LWC standardization process in 2019. It initiated a competition inviting submissions of lightweight cryptographic algorithms for evaluation and standardization. The competition aims to develop and select a set of standardized LWC algorithms that meets specific security and performance requirements.

- ISO/IEC Standards: ISO and the International Electrotechnical Commission have been working on standardizing lightweight cryptography algorithms through various technical committees and working groups. ISO standards play a vital role in ensuring global adoption and interoperability of cryptographic techniques.

- European Telecommunications Standards Institute has been involved in standardizing lightweight cryptographic algorithms for specific use cases, particularly in the context of IoT security and secure communication protocols.

- IETF is the organization responsible for developing and promoting internet standards, has also been involved in discussing lightweight cryptography and its potential applications in various internet protocols and applications.

- Crypto Forum Research Group (CFRG): The CFRG has been actively discussing and evaluating various cryptographic primitives, including lightweight algorithms for potential standardization.

- IEEE Standards Association (IEEE-SA): IEEE-SA is involved in the development of standards for lightweight cryptographic algorithms, particularly for applications in areas such as IoT security and communications.

It is important that standardization efforts take time and involve rigorous evaluation and scrutiny of the submitted algorithms to ensure they meet the necessary security requirements. The NIST LWC competition has been actively evaluating the submitted algorithms and the final selection of standardized LWC algorithms is expected to be a significant milestone.

There are many lightweight algorithms based on Substitution-Permutation Network (SPN)(Chander, S.,2022). PRESENT (Bogdanov, A., et al., 2021) based on SPN structure, uses 64-bit block with 80- bit and 128-bit key variants. PRESENT has round key generation layer, substitution layer and permutation layer. It has 4-bit fixed or static S-Box which makes attacker easy to do attack on a single set of S-Box. RECTANGLE (Zhang, W., et al., 2021) is a lightweight block cipher with the operations like AddRoundKey, Substitution Column and Shift Row. The total number of rounds are reduced to 25. GIFT (Banik, S., et al., 2017) is simple with faster key scheduling algorithms. Two versions of GIFT are: GIFT-64 with 28 rounds having 64-bit block size and GIFT-128 with 40 rounds having 128-bit block size.

Both uses 128 bits key. PRINCE (Borghoff, J., et al., 2012) is a SPN NETWORK which performs 64-bit input utilising 128-bit key. PRIDE (Albrecht, M. R., et al., 2014) has 20 rounds with the introduction of linear layer which makes PRIDE more efficient. So, all lightweight cryptographic algorithm uses fixed or static S-Box which permits attackers to find the weak points of the algorithm.

Simon and Speck (Dwivedi, A. D et al., 2023) are families of lightweight block ciphers developed by the National Security Agency. They are designed to be highly efficient on resource-constrained devices, such as embedded systems and IoT devices. Simon supports block sizes of 32, 48, 64, 96, and 128 bits, while Speck supports block sizes of 32, 48, 64, 96, and 128 bits as well. (El-Hajj, M et al., 2023)., introduced lightweight block ciphers that offer a balance between security and efficiency. KATAN supports key sizes of 64, 80, 96, 104, and 128 bits, while KTANTAN supports key sizes of 80, 128, 192, and 256 bits. These ciphers are suitable for lightweight applications and

constrained environments. (To'xtajon,Q.et al., 2023) introduced a lightweight message authentication code algorithm designed for efficient implementation on devices with limited resources, such as low-power microcontrollers. It provides authentication and integrity for data without requiring heavy computational resources.

(Xiao, L et al., 2020) is a family of lightweight block ciphers that focuses on efficient implementations and resistance against various attacks, including differential and linear cryptanalysis. It supports block sizes of 64 and 128 bits, and key sizes of 64, 128, and 256 bits. MIDORI (Mishra, R et al., 2023) is a family of lightweight block ciphers that come in different versions, including MIDORI64 and MIDORI128. These ciphers aim to provide lightweight implementations while maintaining a high level of security. MIDORI operates on 64-bit blocks and supports key sizes of 64 or 128 bits.

CLEFIA (Saba, S.J et al., 2023) is a lightweight block cipher developed by Sony Corporation. It operates on 128-bit blocks and supports key sizes of 128, 192, or 256 bits. CLEFIA is designed to provide security while maintaining high efficiency on various platforms. TWINE (Chatterjee,K et al., 2022) is a lightweight block cipher that aims to provide efficient implementations on resource-constrained devices. It supports block sizes of 64 and 128 bits, and key sizes of 80, 128, or 160 bits. TWINE is known for its simplicity and low memory footprint. HIGHT (Nayancy,D et al., 2022) is a lightweight block cipher that operates on 64-bit blocks and supports key sizes of 128 bits. It is designed to be highly efficient in both hardware and software implementations while providing security suitable for lightweight applications. FEW (Xiao,H et al., 2022) is a lightweight encryption algorithm specifically designed for wireless sensor networks. It focuses on efficiency and low resource consumption, making it suitable for energy-constrained devices. FEW provides both encryption and authentication functionalities.

There are many mathematical methodologies for the generation and creation of S-Box. (Prathiba, A.,et al., 2018) emphasized the importance of lightweight secure S-Box architectures for the IoT devices. (Wu.et al., 2011) uses the methodology of Latin

square to generate S-Box. S-box based on a fractional linear transformation for image encryption has been proposed by (Farwa S. et al., 2016) But many of these lacks perfect cryptographic properties. (Patidar, V. et al., 2009) used chaotic logistic map to generate pseudorandom numbers. (Ferdush, J., et al., 2021) proposed a standard framework and algorithm based on Arnold and logistic chaotic maps for lightweight image encryption. (Rahman, Z.et al., 2022) used chaos and logistic Map-Based Key Generation Technique for Advanced Encryption Standards. (Masood, F. et al., 2022) proposed the use of Henon chaotic map, Brownian motion, and Chen's chaotic system for encrypting medical images. So, chaotic logistic map has perfect cryptographic properties and can be used to generate a non-linear pseudorandom number. (Shah T. et al., 2019) analysed the power of the proposed S-box through the manipulation of balance property, nonlinearity both differential & linear approximation probability and stringent avalanche criterion. (Panchami, V. et al., 2023) analysed parameters of S-Box of various Lightweight cryptographic algorithms. (Chen, J., et al., 2022) has done an analysis of software and hardware performances of lightweight 8-bit S-Boxes. (Panahi, P.,et al., 2021) discussed the specific encryption performance parameters of lightweight cryptographic algorithms.(Wang, Y.,et al., 2015) used the parameters like non-linearity, linear cryptanalysis for measuring the performance of S-boxes.

2.3.2. Cryptanalysis of Lightweight Cryptography Algorithms

Cryptanalysis involves the study of cryptographic algorithms to identify potential vulnerabilities, weaknesses or security flaws that could be exploited by attackers. The goal of cryptanalysis is to assess the strength and security of LWC algorithms, ensuring it can withstand various types of attacks. Cryptanalysis of LWC algorithms typically covers several key areas:

- Differential Cryptanalysis: This involves analysing how the algorithm behaves when small differences are introduced in the plaintext or the key. Differential cryptanalysis aims to identify possible patterns or biases that could compromise security.

- Linear Cryptanalysis: Linear cryptanalysis seeks to exploit linear approximations in the algorithm to recover parts of the key.

From the literature survey, we could conclude that fixed or static S-Box can permit the attacker to explore S-Box and identify weaknesses of the algorithm. Key dependent approaches are better because it impedes an attacker from any offline analyses of attacks on a S-Box. It is also vulnerable to differential and linear attacks. Static S Box does not possess superior diffusion and does not have a good rate of avalanche effect. So it is important to rectify the security threats explained above to secure the communication between IoT devices and platform.

2.4 SUPPLY CHAIN MANAGEMENT

Supply chain deals with the transfer of goods and data between suppliers, manufacturers, distributors, retailers and consumers. Current supply chains allow business to be integrated thereby minimize loss, increase resources, improve market time, and maintain consumers. The success behind supply chain lies in how effective the activities co-ordinate among the holders and thereby increasing the efficiency of the system. Nevertheless, the supply chains of various farms or agro-enterprises are riddled with difficulties resulting from the agricultural sector's inherent problems. The agri-supply chain network is determined by various challenges such as lack of market requirement data, demand for small quantity, lack of transparency, inadequate storage capacity and poor transportation. The stages of supply chain management is shown in Figure 2.7.

Latest technologies like RFID tag, wireless sensors for tracking and tracing of raw materials have been recognized and tested in the food industry (Zhou, W., et al., 2015). In order to achieve privacy and end-end security, symmetric and asymmetric algorithms are designed to meet the possible attacks like denial-of-Service attack (Elleithy, K. M., et al., 2005), man-in-the-middle attack (Bhushan, B., et al., 2017) and eavesdropping attack (Dai, H. N., et al., 2016).

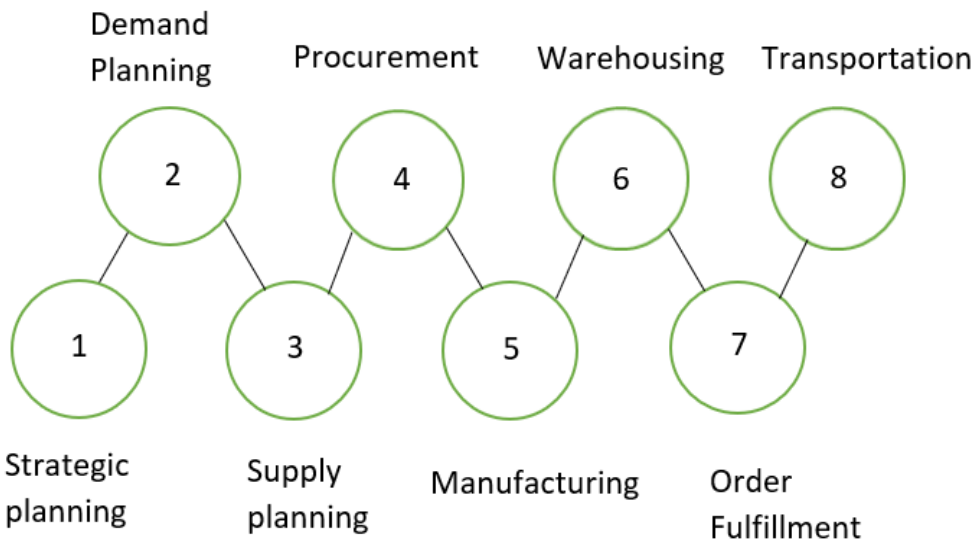

Figure 2.7 Stages of Supply Chain Management

Supply Chain Management involves integrated planning, execution, coordination and monitoring of all business processes and operations necessary to produce and deliver products that meet market criteria as shown in Figure 2.7 (Richey, R. G., et al., 2022). The supply chain is responsible for the movement of food materials and information starting from suppliers and ending with consumers. Supply Chain Management is an approach for optimizing corporate processes and making them more resilient, agile and competitive (Birkel, H., et al., 2021) The cold chain business has gained prominence in recent years with the technological improvements and global economic changes, resulting in increased demand for products.

2.4.1. Challenges in Supply Chain Management

Supply chain connects supplier, manufacturer, distributor and consumer in food industry. The various challenges in supply chain management can be broadly categorized into (i) Technical, (ii) Risk Management, (iii) Performance Measurement and Business Operating Environment (Gurtu, A., et al., 2021), as shown in Figure 2.8.

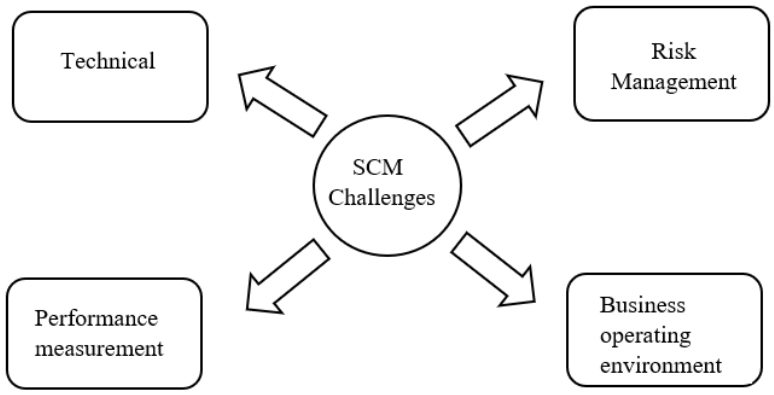

Figure 2.8 Supply Chain Management Challenges

In paper (Zhang, Y., et al., 2017), considering B2B supply chain system models (Haulder, N., et al., 2019), specifically in cold chain networks, some of the core challenges are application integration, environmental factors, operation flexibility, security, trust, data transparency, inadequate temperature monitoring and maintenance system and lack of the latest technology or equipment. (Ashok,A.,et al., 2017) proposed the use of dial thermometers and data loggers to monitor environmental factors, but the limitation is that it does not provide real-time and instant data. (V rat et al., 2018) suggested devices like paper-based temperature monitors that are typically supplied as part of a cold room to monitor internal refrigerator temperatures, but damage to sensitive indicators may fail to measure the temperature. (Aziz, M. A et al., 2018) reported Enterprise Resource Planning software and third-party logistics for Supply Chain Management Operations. A study on IoT-enabled process integration (Novais, L.,et,al,2019) for supply chain management (De. Vass., et al., 2018) is also highlighted, as are the basic issues in supply chain management. However, a simple, secure IoT architecture for small-scale cold chain applications is now unavailable. There are many commercially available (Haddara, M., et al., 2022) Enterprise Resource Planning (ERP) software and third-party logistics for SCM Operations. Third-party logistics has limitations such as skilled talents and trustworthy third parties. The range of functionalities offered by SCM Software Packages have been explored. NetSuite and

Microsoft Dynamics 365 are Cloud based ERP software for small and mid-size business organizations. SAP S/4HANA Cloud is a fully integrated ERP system for large organizations with built-in cognitive technologies such as artificial intelligence, machine learning and advanced analytics. Infor Cloud Suite provide breadth of capabilities for specific industries like retail, healthcare organisations. The drawbacks of ERP software packages for SCM are expensive, vendor-dependent, time-consuming and complex.

SCM has enormous business potential in current world (Dulababu T.,et,al,2018),(Patil,M,.et al., 2015). Within that Cold Chain industry has bigger role to play in the day today life. Cold Chain is a necessity for fish processing, poultry and meat products, dairy, pharmaceuticals etc. There is significant growth in production of perishable products like fish, fruits, vegetables, meat and poultry products and this can be achieved only with improved supply chain system.(Dadhaneeya, H.,et al., 2023) The movement of temperature-controlled products along a supply chain using chilled packaging solutions to protect the quality of products such as fresh agricultural goods, seafood, frozen food, or pharmaceutical products is referred to as cold chain logistics (Mercier, S. et al., 2017). Apache JMeter (Suryadevara, S.,et al., 2020) is a testing tool used to analyse and measure the performance of web applications.

The global market size of cold chain logistics is shown in Figure 2.9. As shown, it starts with a market size of 159 billion US dollars in 2018 and may result in 585 billion US dollars by 2026.

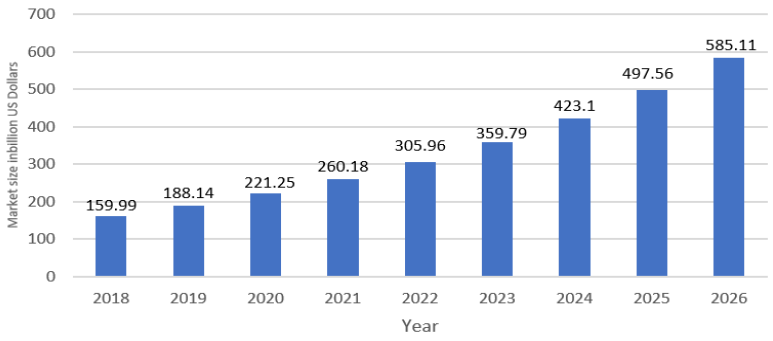

Figure 2.9 Global market size of cold chain (Source: https://www.statista.com)

Fish is easily perishable commodity and its quality get spoiled very quickly. Implementation of Cold Chain industry with latest technology is very critical to maintain the fish quality. Supplier, manufacturer, distributor, retailer and consumer are the entities in Fishing industry. Some of the parameters like temperature, humidity, time to delivery has to be taken care in the cold chain industry. All the entities in the cold chain specifically for fish industry, should have the facility to monitor environmental factors like temperature and humidity.

For instance, assume that the overall throughput time (Althoubi, A., et al., 2021) of the fish pipeline is as indicated in Figure 2.10. The pipeline starts with fish catch and takes one week time when catch arrives and reaches the consumer within 8-20 weeks' time. These 8 to 20 weeks are crucial for the business process and therefore, effective monitoring the key parameters for subsequent decision-making, is essential to improve the efficiency of the cold chain. Otherwise, in case of any adversaries, the period of 8 to 20 weeks would become too large a period for profitable recovery.

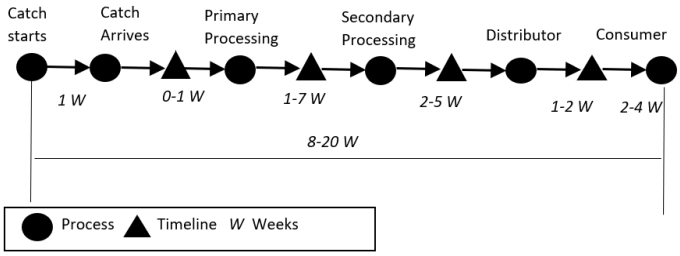

Figure 2.10 An illustration of overall throughput time of the fish pipeline

Some of the problems encountered by supply chain management include careful stock handling, mismanagement of data and live monitoring of products throughout the logistics chain. There are many problems with current systems used in the Supply Chain field. Elements currently leave their data scattered across various supply chain databases and eventually end up losing access to old data. Live monitoring of perishable products like frozen food, meat in supply chain & logistics are undetected. In the healthcare sector, there is an urgent need to monitor and maintain optimum in-transit parameters like

temperature, route and time sensitivity. Internet of Things is one of the emerging optimal solutions to overcome these challenges. IoT can allow real-time visibility of Supply Chain Management where the people in the chain can track the inventory at any given time point using a web/mobile application.

Studying the essential requirements (Mohan, A., et al., 2023) of SCM for small-scale cold chain applications involves understanding the unique challenges and considerations associated with maintaining the temperature-controlled storage and transportation of perishable goods in a limited-scale setting are discussed.

2.5. CHAPTER SUMMARY

The main challenges in SCM for small-scale cold chain applications like food industry have been studied in detail. Importance of retaining the quality of food while transporting from supplier to consumer are discussed. IoT technology can be integrated into existing supply chain marketing and logistics sector thereby improving the services of products. Conventional cryptographic algorithms are not a better choice for resource constrained devices. It is important that the suitability of the lightweight algorithms depends on the specific requirements and constraints of the application. During selection of algorithm, it is recommended to assess the security features, performance characteristics and any available analyses or evaluations.