# CHAPTER 1

# INTRODUCTION

## 1.1 OVERVIEW

Today, Internet of Things (IoT) envisions the autonomous interaction of pervasive and connected, smart nodes that can offer a myriad of services. IoT devices like sensors and actuators are deployed for collecting data from various sources. These devices can gather information about environmental conditions, machine performance and customer behaviour. Real-time data monitoring using IoT can offer valuable insights to enable prompt decision-making based on latest information. As IoT devices are increasingly prevalent in homes, businesses, and critical infrastructure, the IoT nodes are turning into a goldmine of data for malicious actors. Hence ensuring their security is essential to safeguard privacy, maintain operational integrity and prevent potential harm. Today, security and the detection of compromised nodes have become a major concern in IoT networks.

Supply chain management (SCM) encompasses all ensuing activities in the movement and management of materials, products, and information throughout the entire network. Its primary goal is to optimize the overall performance and competitiveness by reducing costs, enhancing customer satisfaction, and improving efficiency. Key components and activities involved in SCM include Planning, Sourcing, Production, Transportation, Warehousing, Inventory management, Distribution, Information systems, Risk management and Collaboration and Communication. SCM has become increasingly important in today's globalized and interconnected business environment. Effective SCM can result in improved efficiency, faster time-to-market, increased profitability, and greater resilience in the face of disruptions.

In temperature - controlled supply chain system or ‘cold chain network,’ some of the core challenges are impact of environment, security in cold chain network, insufficient monitoring and controlling system, absence of modern technology or optimal equipment.

SCM encompasses various activities and processes that can have environmental impacts throughout the entire supply chain. Monitoring the environmental parameters and controlling the flow of products throughout the supply chain is essential for maintaining product quality and ensuring compliance with regulations. Supply chain managers need to implement robust monitoring and controlling systems at various stages, such as production, warehousing, and transportation. Real-time data monitoring and alert systems enable quick response to any deviations, allowing proactive measures to be taken, such as adjusting storage conditions or rerouting shipments to avoid unfavourable environmental conditions.

Security is a crucial concern in today's world, especially when it comes to digital data sharing. With the increasing reliance on digital systems and interconnected networks, data breaches have become a significant concern. Breaches in SCM systems can result in the theft of sensitive information. Conventional cryptography and lightweight cryptography 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 like 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, like embedded systems, IoT devices, and low-power microcontrollers. 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.

To meet the aforementioned requirements, a simple and secure IoT architecture for small-scale cold chain applications is required. In this research work, one such architecture is proposed for integrating IoT sensors with cloud technology for pervasive access of the real-time data in a cold chain environment. The proposed model is demonstrated with a simple web-based working model that has been developed and evaluated. For the security purposes, a dynamic key dependent security algorithm has been developed for which novel

non-linear Substitution Box (S-Box) are generated using Logistic Chaotic Map and evaluated.

## 1.2 MOTIVATION

Small scale cold chain applications normally have automation or high-end technology solutions that is not affordable for small business people. A simple and secure IoT architecture is required for monitoring real time data and controlling the product quality using web-based access for small-scale cold chain applications for better business. Security risk in cold chain network can impact its integrity and auditability and conventional encryption algorithms are not effective enough to be incorporated in the secure transmission of data in resource constrained devices. It is necessary to address the drawbacks of fixed or static S-Box used in cryptography algorithms for devices with limited resources. There is a need to enhance the data security levels by generating non-linear Substitution Boxes(S-Boxes) through dynamic key dependent algorithm.

## 1.3 PROBLEM DEFINITION

Logistic constraints, inaccessible warehouses, and closed consumer outlets, during COVID-19 pandemic, affected supply chains especially in small scale cold chain sectors. This brings out the need for simple and small-scale technological solutions that could monitor, manage, secure, and facilitate decision-making for reducing losses. The solution must be capable of making use of the IoT's in the pervasive smart phones that almost everyone in the unorganized sector of small businesses, is possessing. It must be able to integrate the power of cloud storage with the data handling capacity of hand-held devices via the Internet as the backbone in a feasible manner. Securing data becomes an essential requirement in such situations, thus simple security algorithms must be a part of the solution to be provided. Further for data collection during transit, smart containers with sensors are to be made an integral part of the system. Small business firms could then monitor, track, and receive notifications about their goods as they moved along the cold chain.

## 1.4 RESEARCH OBJECTIVES

The primary objective is:

- To model a simple, secure integrated IoT architecture which provides real-time data handling in a cold chain environment using a Cloud based web application.

The secondary objectives are:

- To evaluate and demonstrate the proposed architecture with a web-based working model.
- To propose a dynamic key dependent cryptographic algorithm for securing communication between IoT devices and web application.
- To generate and evaluate novel non-linear S-Boxes using Logistic Chaotic Map for the dynamic key dependent cryptographic algorithm.

## 1.5 SCOPE

The research work is providing a holistic approach for SCM entities with a simple, secure integrated IoT architecture which provides real-time data handling for small scale cold chain applications using a Cloud based web application. The cold chain entities can monitor the commodity with real-time data handling capabilities, secure transactions, web-based access to the system, mobile App for role-based access to the system for the end-users, and alerts and notifications regarding the goods in the chain.

The model is meant for small scale business and therefore does not include high-end IoT systems nor does it include the complete spectrum of precision sensors that are common in commercially available SCM's. Features that are essential for full-fledged commercial SCM's such as fault tolerance, storage management, intensive data analytics, etc., are not considered as essential for the given scenario, thus making the system simple, economical, and feasible for small businesses. The model does not include commonly used hardware components and devices.

## 1.6 CONTRIBUTIONS

The major contributions which bring novelty to this research are listed below:

- A web-based working model is developed to demonstrate the integrated IoT architecture
- A simple, robust open-source implementation platform is identified and evaluated to handle real-time data and provide a runtime environment for server-side web applications
- A prototype beta version of app has been developed to make use of common sensors available in the market
- A dynamic key dependent algorithm for the secure transmission of data between IoT devices and web application is developed and evaluated
- Non-linear S-Boxes using Logistic Chaotic Map for the dynamic key dependent cryptographic algorithm are generated and evaluated

## 1.7 ORGANIZATION OF THE RESEARCH WORK

**Chapter 1** describes overview, motivation, problem definition, research objectives, scope, and contributions.

**Chapter 2** discuss existing studies on IoT architecture, challenges, cold chain, conventional cryptography, lightweight cryptography with their related limitations.

**Chapter 3** describes the proposed integrated architecture along with its results and evaluation.

**Chapter 4** discuss the generation of non-linear S-Boxes and its results. The chapter explains the selection of dynamic key dependent S-Boxes, used to develop the novel lightweight cryptographic algorithm with its results. This chapter illustrates the overall experimental evaluation results to prove effectiveness of proposed algorithm.

**Chapter 5** concludes the research findings with outlines for future enhancements and reference part with list of evidences used to explain the related concepts of the proposed methodology.

## 1.8 CHAPTER SUMMARY

This chapter gives an overview of IoT, supply chain management, cryptographic systems. Then, the need for a simple, secure IoT architecture for small scale cold chain applications is discussed. The chapter also discuss with the scope, list of objectives of the proposed architecture along with deliverables, contributions in the research to enhance the security in the IoT systems and concludes with the organization of the thesis.