# SPECIMEN FORMAT FOR THESES OF MONTH

| | | |
|---|---|---|
| Faculty | : | School of Engineering |
| Department | : | Computer Science & Engineering |
| Branch/ Area: | : | IoT Security |
| Sub Subject Heading: | : | - |
| Candidate's Name | : | Divya James |
| Candidate's Address with email | : | BLISS,32/1165<br>NETTAIKIDATHU ROAD<br>PALARIVATTOM<br>COCHIN-25 |
| Title of the thesis | : | SiC-Chain: A Simple, Secure IoT System Architecture for Small Scale Cold Chain Applications |
| (i) In Roman Script<br>(ii) In roman Script | | - |
| Nomenclature of Degree: | : | Ph.D |
| Month & Year of Enrolment: | : | January 2019 |
| Month & Year of Registration: | : | January 2019 |
| Month &Year of Submission: | : | October 2024 |
| Month &Year of Award | : | March 2024 |
| Name of Supervisor | : | Dr.TKS.Lakshmi Priya |
| Designation of Supervisor | : | Former Professor,Department of Printing Technology |
| Centre/department/school in which research was conducted | : | School of Engineering |
| University's Name & Address | : | Avinashilingam Institute for Home Science and Higher Education for Women, Coimbatore,641043 |

**Abstract within 300 words:**

Supply Chain Management involves the coordination and management of various interconnected activities and processes across different organizations and functions within a supply chain. Real-time monitoring, efficient data handling and secure business transactions are vital for effective operations of supply chain management. As regards, temperature-controlled supply chain system or 'cold chain network' there arise certain core challenges. Extraneous factors could impact the operating environment. Security risk in cold chain network can affect the supply chain's integrity and auditability. Our proposed layered architecture – "SiC-Chain" provides real-time data collection, seamless storage, and secure communications for cold-chain applications. SiC-Chain architecture has been designed with three types of operations namely SiC-Chain Enrollment, SiC-Chain transactions and SiC-Chain Secure IoT.For implementation of SiC-Chain, the fishing industry has been identified as an application. For real time monitoring, a smart IoT device named 'SiC-SBox' has been developed. A user-friendly web-based application that can be used on mobile devices has been created to provide access to the SiC-Chain system. A SiC-Chain prototype development environment consist of SiC-SBox, SiC-Chain Backend on the Cloud and SiC Chain Application with a smart Dashboard has been developed and evaluated.

To address the concern of secure transactions within the supply chain management entities, SiC-Chain architecture employs a novel dynamic key dependent cryptographic algorithm. This algorithm selects non-linear S-Boxes dynamically based on the round key generated for each round. By using cryptographic techniques, the architecture provides a secure communication channel for transmitting the sensor data to web application. Experimental results and evaluation show that encryption of IoT data using the algorithm can contribute to the security of cold chain applications and ensure the confidentiality of transmitted data. The performance analysis has been done on encryption time, decryption time, strict avalanche effect, throughput, and memory consumption. The novel nonlinear S-Boxes used in SiC-Chain architecture was screened for non-linearity, Differential and Linear approximation probability analysis which showed excellent outcomes compared to other lightweight algorithms.

**i) Major 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.

### ii) Hypothesis:

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.

### iii) Methodology :

The thesis work primarily involves the proposal of an IoT architecture for cold chain environment catering to small scale businesses in Indian scenario. As depicted in Figure 3.1, the research methodology adopted for the work in the thesis is described below:

**1. Initial Study-** The first step is the study of the essential requirements of SCM for small businesses dealing with goods that are temperature sensitive. The architecture incorporates features like use of simple and easily available sensors-based systems, real-time data handling capabilities, web-based access to the system, mobile App for role-based access to the system for the end-users, alerts and notifications regarding the goods in the supply chain.

**2. Modeling the SiC-Chain architecture**-. 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 SCMs. Features that are essential for full-fledged commercial SCMs such as Fault tolerance, storage management, intensive data analytics etc, are not considered essential for the given scenario, thus making the system simple, economical, and feasible for small businesses.

**3. Setting up the implementation platform**- To demonstrate the architecture, a working model is developed for which a suitable implementation platform was first chosen. The platform was chosen to be open source, asynchronous, event driven, fast in code execution and provide a runtime environment for developing server-side web applications. The platform was chosen to be able to handle the IoT data in real-time, in a secure manner, must support a lightweight desktop environment and mobile end users, real time data analysis and a database that is distributed and optimized for fast growing web and mobile apps.

**4.Testing the platform-**Before finalizing a suitable platform, an experimental setup of a simple IoT system with a few sensors was used for real-time, encrypted data collection and uploading to web-based platform. This setup also included a lightweight desktop environment for handling the sensors as well as for computational tasks. The setup along with the identified platform was then used for analysing the real-time data.

**5. Developing a web application**-After testing with larger data sets, a full-fledged web-based application, with pairing mobile apps for end users, has been developed and tested. The development platform has been designed to handle the view layer used for development of both web and mobile applications. The performance evaluation for web application was analysed and average response time for transactions was calculated to verify acceptable performance levels.

**6. Developing non-linear S-Boxes**- After developing the platform and evaluating it, the next step was to develop novel non-linear S-Boxes, the basic building boxes of the cryptographic algorithm, using Logistic Chaotic Map. Performance analyses of S-Boxes were executed on non-linearity and on both Differential and Linear Approximation Probability.

**7. Developing a Dynamic Key Dependent algorithm** -To further improve the security of web-based application a light weight dynamic key dependent security algorithm for secure communication between the IoT devices and the web application was developed. Dynamic key dependent cryptographic algorithm has been chosen for this purpose and performance evaluation parameters like strict avalanche effect, average encryption and decryption time, throughput, and memory consumption time were determined.

**8. Overall System Testing** - The platform was subjected to larger data sets and the entire system was evaluated. Since no benchmark datasets exist for environmental parameters, the platform has been demonstrated with a dataset consisting of sensor data with the experimental readings taken during multiple trails at different time intervals.

**iv) Findings:**

A simple, secure integrated IoT architecture named as 'SiC-Chain' has been developed which provides real-time data handling in a cold chain environment. This layered architecture enables SCM entities in cold chain to take suitable decisions easily. Typically, the SiC-Chain architecture division into layers promotes modularity, scalability, security, simplified development, flexibility, and ease of maintenance. The three types of operations for SiC-Chain architecture namely SiC-Chain Enrollment, SiC-Chain transactions and SiC-Chain Secure IoT has been implemented and fishing industry for small businessmen has been taken as the sample application for implementing SiC-Chain. A smart IoT device – 'SiC-SBox,' cloud-based data processing and storage system- SiC-Chain Backend on the Cloud, with a user-friendly smart SiC-Chain dashboard has been developed for small scale cold chain applications. The three modules of SiC-Chain architecture namely SiC-SBox, SiC-Chain Backend on the Cloud and SiC Chain Application with a smart Dashboard has been tested and evaluated. SiC-SBox has been functionally tested for interfacing and data collection, processing, and transmission. By measuring the average response time, the operations of SiC-Chain backend on the cloud have been tested. Finally, the SiC-Chain application has been tested for its functionality, interface, useability, database, and compatibility.

A non-linear S-Boxes, the basic building boxes of the cryptographic algorithm, using Logistic Chaotic Map are generated. To further improve the security of web-based

application, dynamic key dependent algorithm is developed. The data between the IoT devices and platform in SiC-Chain architecture has been securely transferred using a dynamic key dependent algorithm. The performance evaluation of non-linear S-Boxes is evaluated based on non-linearity, both Differential and Linear Approximation Probability and Dynamic key dependent algorithm is evaluated based on strict avalanche effect, average encryption/decryption time, throughput and memory consumption. Through

**Examiners**

**Internal Examiner :** Dr. V. Mary Anita Rajam
Professor
Department of Computer Science & Engineering,
College of Engineering Guindy
Anna University,
Chennai - 25.

**External Examiner :** Dr.Xavier Fernado

Professor and Director

Toronto Metropolitan University,Canada