**AES Encryption for Allergen-Safe Cosmetic Manufacturing Process on Supplier Containers**

**PREFACE**

**TABLE OF CONTENTS**

**1. SOFTWARE DEVELOPMENT LIFE CYCLE**

**2. PLATFORM KNOWLEDGE**

**3. DOMAIN KNOWLEDGE**

**4. ABOUT PROJECT**

4.1 ABSTRACT

4.2 SCOPE OF THE PROJECT

4.3 EXISTING SYSTEM

4.3.1 DISADVANTAGES

4.4 PROPOSED SYSTEM

4.4.1 ADVANTAGES

**5. BOTTOM LINE AND FUTURE ENHANCEMENT**

**6. SOFTWARE AND HARDWARE REQUIREMENTS**

**1. SDLC (Software Development Life Cycle)**

The Software Development Life Cycle is a systematic process for building software that ensures the quality and correctness of the software built. SDLC process aims to produce high-quality software which meets customer expectations. The software development should be completed within the pre-defined time frame and cost.

**SDLC Phases**

The entire SDLC process is divided into the following stages:



* Phase 1: Requirement gathering and analysis
* Phase 2: Feasibility Study
* Phase 3: Design
* Phase 4: Coding
* Phase 5: Testing
* Phase 6: Installation/Deployment
* Phase 7: Maintenance

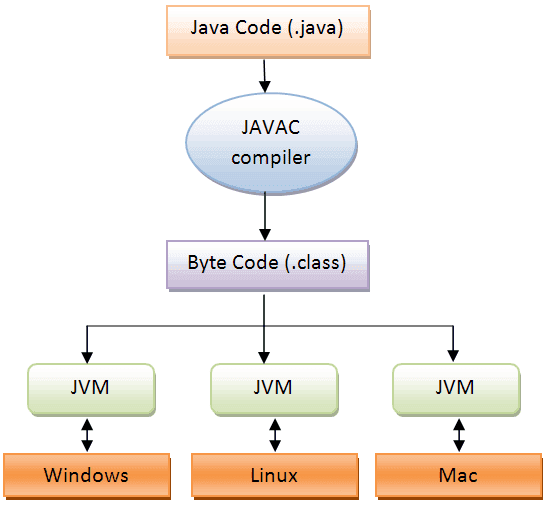
**2. PLATFORM KNOWLEDGE**

**Introduction to java**

Java programming language was originally developed by Sun Microsystems which was initiated by James Gosling and released in 1995 as a core component of Sun Microsystems' Java platform. Initially, the language was called “Oak” but it was renamed as “Java” in 1995. The primary motivation of this language was the need for a platform-independent language. Finally, Java is for Internet Programming where C was to System Programming.

**Java architecture**

Java is a high-level Object-oriented programming language. A program written in high level language cannot be run on any machine directly. First, it needs to be translated into that particular machine language. The javac compiler does this thing, it takes java program (.java file containing source code) and translates it into machine code (referred as byte code or .class file). Java Virtual Machine (JVM) is a virtual machine that resides in the real machine (your computer) and the machine language for JVM is byte code. JVM executes the byte code generated by compiler and produce output. JVM is the one that makes java platform independent.

****

**3. DOMAIN KNOWLEDGE:**

**Cybersecurity:**

Cyber security, short for "cyber security" or "cyber security," refers to the practice of protecting computer systems, networks, devices, and data from theft, damage, unauthorized access, and other forms of digital threats. It encompasses a wide range of technologies, processes, practices, and measures designed to safeguard information technology (IT) systems and the data they store or transmit.

**Key components of cybersecurity :**

**Information Security:** Protecting the confidentiality, integrity, and availability of data is a fundamental aspect of cybersecurity. This involves encrypting sensitive information, controlling access, and ensuring data remains unaltered.

**Application Security:** Ensuring the security of software applications by identifying and mitigating vulnerabilities that could be exploited by attackers.

**Identity and Access Management (IAM):** Managing user and device access to systems and data, often through authentication methods like usernames and passwords or more advanced techniques like multi-factor authentication (MFA).

**Security Awareness and Training:** Educating employees and users about security best practices and potential threats to reduce human error and susceptibility to social engineering attacks.

**Incident Response and Recovery:** Preparing for and responding to security incidents, breaches, or data losses, including investigation, containment, and recovery.

Cybersecurity is essential in today's digital world because of the increasing frequency and sophistication of cyberattacks. The consequences of security breaches can be severe, leading to financial losses, damage to reputation, and legal implications. It is an ongoing effort that requires constant vigilance and adaptation to address the evolving threat landscape.

**4. ABOUT THE PROJECT**

**4.1 Abstract**

In response to the contemporary need for enhanced transparency and quality assurance within the cosmetic industry, we are pioneering a groundbreaking approach to cosmetic manufacturing. This innovative system seamlessly integrates the cutting-edge technology of block chain, fortified by the formidable SHA-512 encryption standard and the robust AES encryption. Together, these security measures create a highly secure and completely transparent production process for cosmetics. SHA-512, which stands for "Secure Hash Algorithm 512," is a cryptographic hash function. It is part of the SHA-2 (Secure Hash Algorithm 2) family of encryption algorithms and is designed to produce a fixed-size 512-bit (64-byte) hash value from any input data, making it extremely secure and resistant to collisions (two different inputs producing the same hash).Every stage of cosmetic creation, from initial formulation to rigorous testing, is meticulously recorded within the block chain’s immutable ledger, guaranteeing a level of data integrity and security that is second to none. Furthermore, this system goes beyond merely securing the production process; it extends its transparency to encompass the sourcing of containers, thereby reinforcing trust and accountability in the world of cosmetic manufacturing. This comprehensive approach sets new industry standards, ensuring that customers can be confident in the quality and authenticity of the products they use, while simultaneously enhancing the integrity of the cosmetic manufacturing process.

**4.2 SCOPE OF THE PROJECT:**

The scope of this project encompasses a comprehensive transformation of the cosmetic manufacturing process, introducing cutting-edge technologies and best practices to address the evolving needs of the cosmetic industry. It includes the integration of block chain technology with SHA-512 and AES encryption standards to ensure unparalleled data security and integrity throughout the entire cosmetic production cycle. The project extends its reach to encompass the meticulous recording and secure storage of data pertaining to ingredient sourcing, formulation, quality control, testing, and container supply. Furthermore, it involves the implementation of rigorous microbial testing processes to assess and disclose any potential allergic content in the cosmetic product, thereby enhancing safety and transparency. Additionally, it aims to enhance transparency, trust, and accountability within the cosmetic manufacturing ecosystem, meeting the rising demand for product authenticity, ethical sourcing, and safety. By setting new industry benchmarks, this project is not only poised to meet consumer expectations but also to pioneer a future where responsible, trustworthy, and allergen-safe cosmetic manufacturing practices prevail.

**4.3 Existing System:**

In the traditional cosmetic manufacturing landscape, the industry largely relies on conventional methods of production and record-keeping. Ingredient sourcing, formulation, quality control, and testing processes are conducted using standard protocols with limited data traceability. Data storage primarily involves centralized databases and paper records, leaving room for potential data tampering and security vulnerabilities.The existing system lacks the comprehensive transparency and security that consumers now demand from the cosmetic industry. Ingredient sourcing, though often regulated, may lack detailed information on suppliers and their certifications. The formulation and testing phases are conducted using manual processes, making it challenging to provide complete product traceability. Moreover, the system does not inherently address allergen content, leaving potential gaps in safety and transparency.IN essence, the cosmetic manufacturing industry, in its current state, faces limitations in data security, transparency, and safety measures, which the proposed block chain-based system with microbial testing seeks to address comprehensively.

**DISADVANTAGES:**

* Lack of Transparency: The existing system lacks transparency in the sourcing of cosmetic ingredients, making it challenging for consumers to know the origins and certifications of the components used in their products.
* Data Vulnerability: Data is stored in centralized databases and paper records, making it susceptible to tampering and unauthorized access. This compromises the integrity of critical information related to the production process.
* Limited Traceability: The conventional system does not provide end-to-end traceability of cosmetic products, making it difficult to track the complete journey of a product, from ingredient sourcing to its final destination.
* Inadequate Allergen Testing: Allergen testing is not a standard practice in the existing system, which may result in cosmetic products containing allergens not being properly identified, potentially leading to allergic reactions in users.

**4.4 Proposed System**

Our proposed system represents a revolutionary approach to cosmetic manufacturing, designed to rectify the limitations of the existing system and usher in a new era of transparency, security, and safety. It leverages state-of-the-art blockchain technology, fortified by the impenetrable SHA-512 encryption standard and AES encryption, to create an airtight ecosystem. Every phase of cosmetic production, including ingredient sourcing, formulation, quality control, testing, and container supply, is meticulously recorded and securely stored within the blockchain's immutable ledger.A pivotal enhancement in the proposed system is the introduction of rigorous microbian testing processes. These tests are aimed at identifying and disclosing any potential allergens in cosmetic products, providing consumers with comprehensive information about product safety. The inclusion of allergen testing not only ensures customer well-being but also aligns the cosmetic industry with modern demands for allergen disclosure and safety assurance.

**ADVANTAGES:**

* Enhanced Transparency: The proposed system leverages blockchain technology to provide complete transparency in the cosmetic manufacturing process. Consumers can access detailed information about ingredient sourcing, quality control, and testing, promoting trust and confidence in product authenticity.
* Unprecedented Data Security: With SHA-512 encryption and AES encryption, the proposed system ensures data security and integrity at the highest levels. This greatly reduces the risk of data breaches, tampering, or unauthorized access.
* Allergen Testing: The inclusion of rigorous microbian testing processes enables the identification and disclosure of potential allergens in cosmetic products. This ensures consumer safety and allows individuals with allergies to make informed choices.
* Comprehensive Supply Chain Visibility: The proposed system records and stores information about container suppliers, certifications, and sustainability measures in the blockchain. This comprehensive approach extends transparency to the entire supply chain.

**5. BOTTOM LINE AND FUTURE ENHANCEMENT**

The proposed system marks a transformative shift in cosmetic manufacturing, addressing the limitations of the existing system. By leveraging blockchain technology with robust encryption standards, introducing allergen testing, and ensuring supply chain transparency, it sets new industry standards for transparency, safety, and ethical practices. This innovative approach not only instills trust and confidence in consumers but also positions the cosmetic industry to meet the evolving demands of authenticity and safety. Additionally, advanced microbial testing methods are on the horizon for even more accurate allergen detection. These forward-looking enhancements will elevate cosmetic manufacturing to a new level, ensuring it remains a paragon of responsible, secure, and trustworthy practices in the cosmetic industry.

**6. HARDWARE AND SOFTWARE REQUIREMENTS**

**Hardware requirements:**

* Processor : Intel (R) Pentium (R)
* Speed : 1.6 GHz and Above
* RAM : 4 GB and Above
* Hard Disk : 120 GB
* Monitor : 15’’ LED SVGA
* Input Devices : Keyboard, Mouse

**Software requirements:**

* Operating system : Windows 7 / 8 / 8.1 / 10
* Coding Language : JAVA / J2EE
* Java Version : jdk 8
* IDE : Eclipse Oxygen
* Database : MySQL v5.1
* Database Tool : HeidiSql v11.0
* Application Server : Apache Tomcat 8.X / 9.X