UONGOZI-Journal of Management and Development Dynamics

2024, Vol 34, No. 1, 20-49

ISSN 2619-8665

Bluetooth Low Energy Beacon-based Method for Securing Genuine Products in Supply Chains

Jovin John Kamala[1], Morice Daudi[2]

Received: 01August 2024
Published: 22 December 2025

ABSTRACT

Counterfeit products pose a significant threat to global supply chains, particularly in low-resource settings with limited regulatory oversight. Existing anti-counterfeit solutions often fall short by failing to prevent product ID duplication or engage all supply chain actors. To address these limitations, this study develops a Bluetooth Low Energy (BLE) beacon-based method for securing genuine products and detecting counterfeit infiltration. The method combines geofencing, encryption, and stakeholder inclusivity to ensure products are authenticated only within authorised physical locations. It was implemented as a mobile and web-based system, tested through controlled laboratory experiments, and evaluated using a structured user survey. Experimental results demonstrated the method's effectiveness in detecting counterfeit products and rejecting unauthorised or duplicated scans. User evaluations confirmed high usability, satisfaction, and system responsiveness, with broad support for real-world deployment. The findings highlight the method's potential to democratise counterfeit detection, prevent ID reuse, and reinforce product traceability. Overall, the BLE beacon-based approach offers a practical, scalable, and cost-effective solution to enhance supply chain security and consumer trust.

Keywords: *BLE beacons, counterfeit products, supply chain, counterfeit detection method, counterfeit detection, product history*

[1] Corresponding author, Faculty of Informatics and Technical Education, National Institute of Transport, jovin.kamala@nit.ac.tz

[2] Faculty of Science and Technology, Mzumbe University

1 INTRODUCTION

Nowadays, the markets are so full of genuine and counterfeit products that they confuse customers. Even though the number of market counterfeits may not be precisely known, many customers may have bought them with or without their knowledge. Manufacturers, distributors, shippers, and governmental entities prioritise removing counterfeit goods from the supply chain (Altaf et al., 2022). Though opinions on the scale of counterfeiting vary in this discourse, most consider it a multi-billion-euro global industry (Commuri, 2009). Every country worldwide is impacted by counterfeiting, either at a point of origin, destination or in transit (Plane & Chen, 2016). Counterfeit products include clothing, pharmaceuticals, cosmetics, accessories, beverages, and electronics. The rise in counterfeit products may be attributed to several developments, such as technological breakthroughs that have made it possible for counterfeiters to quickly and inexpensively replicate packaging (Canayaz & Gurun, 2018; Ghadge et al., 2021; Park et al., 2017; Wilson et al., 2016). Estimating the exact level of counterfeiting and the harm it brings to different groups is challenging because counterfeits are produced and sold in markets where they go unregulated, evading average tax and tariff payments (Commuri, 2009; Davison, 2011). Reports about counterfeiting in developing countries are relatively rare and unsatisfactory than those from the most industrialised countries (Davison, 2011). The reason for the underreporting of counterfeit product occurrences might lie in the inadequacies of regulatory frameworks and market oversight in developing nations. Additionally, most product beneficiaries, particularly in lower-middle-income countries, possess limited or insufficient knowledge regarding genuine products (El-Dahiyat et al., 2021). That circumstance underscores the critical importance of sustaining efforts to combat counterfeit products.

Methods for the control and detection of counterfeits cover a variety of strategies that primarily fit into two concise categories: *physical inspections* and *traceability solutions*. The physical inspection involves technology and methods primarily grounded in quality control and authentication procedures. These procedures include visual checks, packaging analysis, and laboratory testing (Asadizanjani et al., 2021; Citti et al., 2018). Other technologies employ specialised tools for the analysis of materials and product components. The physical inspection techniques entail systematically inspecting

physical characteristics to spot any irregularities indicating a counterfeit item. On the other hand, traceability-based solutions often focus on data management, unique identifiers, and tracking systems. Techniques such as QR codes, GPS, IoT sensors, RFID tags, and data analytics play a pivotal role (Agnusdei et al., 2022) in tracing products across a supply chain segment. The methods revolve around creating a transparent and traceable supply chain where product movements can be monitored in real-time, enabling the detection of irregularities or unauthorised product transfers (Lin et al., 2022).

Existing literature has contributed to efforts to remove counterfeits in the supply chain, as highlighted in previous paragraphs. However, to successfully address the vulnerability of products to duplicate or reuse easily, the literature lacks a traceability solution based on inclusive processes capable of establishing a comprehensive and accurate product transactional history. The solution must consider two crucial practices to deliver the best results. First, it must actively engage all feasible supply chain actors to combat counterfeits. Second, it must involve minimising or doing away with obstacles like product duplication, reusing packages, and the expenses related to implementing and managing alternative solutions. To this end, the overall objective of the present paper is to develop a method for detecting counterfeits in the supply chain. The paper contributes by devising a Bluetooth Low Energy (BLE) beacon-based method that involves key stakeholders of a particular supply chain to secure genuine products from counterfeit ones. Also, the method detects infiltration of counterfeit products. The paper answers one research question: *How can a supply chain of genuine products be safeguarded using BLE beacons?* The method combines IoT (beacons), cloud, mobile, and QR technologies to protect the supply chain. The method benefits and involves manufacturers, wholesalers, retailers, and final customers.

1.1 Counterfeits in Brands

Effective brand management enables companies to differentiate themselves and effectively communicate the value of their products and services. Based on contingency theory (Kros et al., 2019), firms adopt strategies in response to internal and external pressures. These may include sales declines, product quality complaints, or third-party reports (Wilson et al., 2016). In such cases, verifying brand authenticity becomes essential, and anti-forgery measures are critical.

Counterfeit brands are widely discussed in the literature. They are defined as products bearing a trademark that is identical to or confusingly similar to one that is legally registered by another party, thereby violating trademark rights (Bian & Moutinho, 2009). In contrast, imitations—also known as copycats, lookalikes, or me-too products—resemble branded items but are not identical (Le Roux et al., 2016). While counterfeits are exact copies of original products, imitations mimic the appearance without replicating the original in its entirety. Understanding this distinction is crucial for enforcing brand protection strategies and preventing consumer deception.

1.2 Methods for Controlling Counterfeits

The literature presents numerous methods to address counterfeiting, which generally fall into six categories: (i) physical inspection, (ii) online verification via databases, (iii) covert methods using special devices, (iv) QR codes scanned by smartphones, (v) overt methods involving visible marks, and (vi) electronic tags like RFID chips. Physical inspection remains widely used but often requires trained professionals rather than ordinary customers. In some cases, it can create distrust between business owners and inspection teams. This method relies on quality control and authentication procedures such as visual inspection, packaging analysis, and lab testing (Asadizanjani et al., 2021; Citti et al., 2018). Agencies like the Tanzania Medicines and Medical Devices Authority (TMDA) and the World Customs Organization's Interface Public Members (IPM) employ such approaches.

The second and third methods involve online verification and covert techniques. The online verification allows users to send a product ID to a central database for authentication. While effective, it can be vulnerable to security breaches, unauthorized database access, or replication attempts (Gonzalez et al., 2014; Zhao et al., 2018, 2019). To enhance security, this method is often integrated with others (Gianmarco et al., 2015). The covert methods involve features that are invisible to the naked eye and require specialized devices for verification. These methods are typically accessible only to brand owners or professionals. For instance, encrypted text visible only under special lighting may be embedded on packaging (Anilkumar et al., 2012; Yuanli et al., 2017). However, most consumers lack awareness or access to the tools required for detection. Companies like Johnson & Johnson Services (2021) and Prooftag (2021) use these methods to protect their brands.

The fourth, fifth, and sixth methods are the QR codes, overt and electronic tags, respectively. The QR codes provide basic product information and are easily scanned by smartphones. However, they are vulnerable to duplication and misuse, including redirection to unauthorized databases. Therefore, QR codes must be combined with other technologies for effective protection (Bansal et al., 2013).

Overt methods rely on visible and easily recognizable marks. While simple to implement, they often require user training, are prone to imitation or reuse, and may provide a false sense of authenticity (Cruikshank, 2014; Gianmarco et al., 2015).

Electronic tags, such as RFID chips, offer robust tracking but can be costly to implement across an entire supply chain. Though the chips themselves are inexpensive, system-wide deployment and maintenance can be high. RFID tags are also susceptible to cloning and raise privacy concerns if not deactivated after purchase (Li, 2013a; Zhao et al., 2018, 2019; Gianmarco et al., 2015).

1.3 Techniques for Detecting Counterfeits

This section identifies and describes critical methods for detecting counterfeits in the supply chain. It is structured into two parts: location-aware technologies (sub-section 1.3.1) and techniques for applying (electronically) to identify a physical object (section 1.3.2).

1.3.1 BLE Beacons as the Location-aware Technology

The detection technology uses location-aware systems to permit access only within authorized premises, helping identify misplaced or misdirected products with minimal impact on user devices. This subsection introduces BLE-beacon technology as an effective solution. A BLE beacon is a low-power radio transmitter that periodically broadcasts signals to nearby devices (Filippoupolitis et al., 2017; Jeon et al., 2018; Sterling et al., 2014; Altaf et al., 2022). Its advantages include low cost, small size, low energy consumption, and wide compatibility with modern devices (Manasreh et al., 2023). Figure 1 presents several beacon device providers available in the market.

Figure 1: Examples of BLE beacons (Source: (Sterling et al., 2014))

The BLE beacons have an edge over GPS services and provide indoor and underground location services; thus, they do not require any satellite (Electronicsforu, 2016). Beacons communicate via Bluetooth Low Energy technology that enables a business to provide certain location-based services to their customers using very little power; they are designed to minimise the impact on the device's battery life (Andreev & Aprahamian, 2018; Wu & Tsai, 2018). A beacon detects only if a Bluetooth-enabled device has entered its zone (Sterling et al., 2014; Wu & Tsai, 2018). Thus, if a device owner has an associated application with the emitted beacon signals, a beacon will initialise the assigned operation or service.

1.3.2 Object Detection

Perception precedes observation; thus, a detector must first recognize the object it is meant to perceive. A detector trained to identify genuine products can determine authenticity. Object detection involves locating instances of known object classes, such as people, cars, or faces, in images (Correa et al., 2012; Felzenszwalb et al., 2010; Verschae & Ruiz-del-Solar, 2015). It is widely used in human-computer interaction, robotics, and consumer electronics (Amit et al., 2020; Verschae & Ruiz-del-Solar, 2015), as well as in image retrieval, security (e.g., recognition and tracking), and transportation for autonomous driving (Correa et al., 2012; Felzenszwalb et al., 2010). In security applications, object detection plays a critical role in preventing and controlling counterfeit products, helping protect public safety, supplier reputations, and brand identity.

A counterfeit product detector should determine authenticity by analyzing embedded security features. Research (Davison, 2011; Gianmarco et al., 2015; Li, 2013b) classifies counterfeit detection technologies into authentication and traceability. Authentica-

tion verifies if a product is genuine, while traceability tracks its movement through the supply chain (Li, 2012; Qian et al., 2011; Ting & Ip, 2013).

a) Authentication Technologies

Authentication technologies are used to verify that a product is genuine. According to literature (Gianmarco et al., 2015; Li, 2013b; Ting & Ip, 2013), authenticity is confirmed through additional security features integrated into the product. These features enable authenticators to assess whether a product is genuine. Authentication technologies are broadly categorized into overt and covert types (Agrawal et al., 2010; Cruikshank, 2014; Gianmarco et al., 2015; Li, 2013b).

Overt technologies are visible to the naked eye and do not require specialized tools, while covert technologies are hidden and need special devices for verification (Agrawal et al., 2010; Bansal et al., 2013; Ting & Ip, 2013). Common authentication technologies include watermarks, holograms, color-shifting ink, security threads, micro-printing, and barcodes (Gianmarco et al., 2015; Ting & Ip, 2013). Others include physical and packaging security technologies, biological anti-counterfeiting, and latent image decrypt technologies. Examples of these technologies are illustrated in Figure 2.

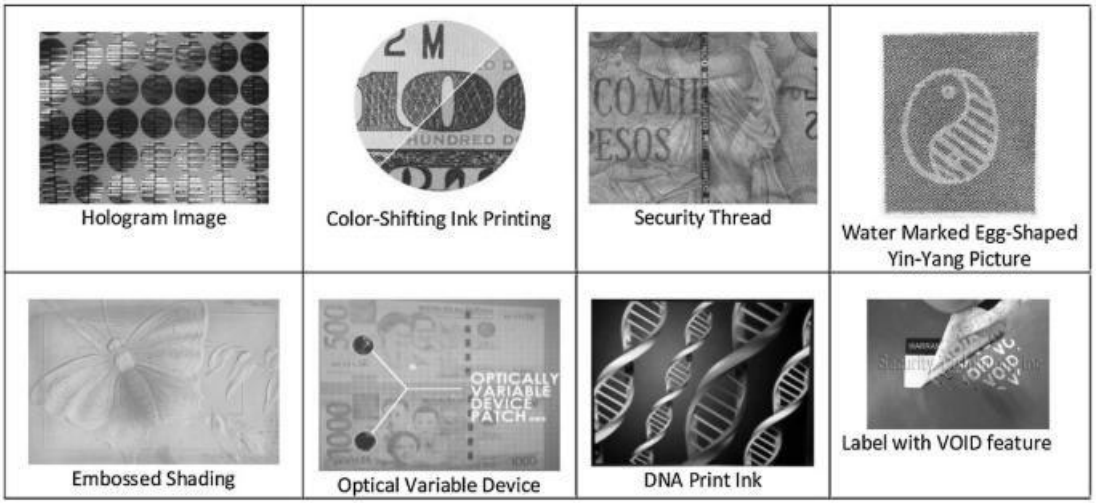

Figure 2: Examples of product authentication technologies (Source: (Li, 2013b))

Challenges with overt technologies include user training requirements, the possibility of reuse or imitations, and the potential for deceptive assurance (Gianmarco et al., 2015; Li, 2013b). Even in cases where the authentication device is managed exclusively by the device supplier, covert technologies are vulnerable to the risk of compromise,

straightforward imitations, and increased costs (Cruikshank, 2014; Gianmarco et al., 2015; Qian et al., 2011).

b) Traceability Technologies

Before reaching the final customer, a product typically passes through multiple actors or intermediaries. This complexity makes it difficult to determine a product's transactional or geographic history during a suspected counterfeiting incident without consulting additional data (Davison, 2011). Traceability technologies address this issue by enabling the tracking and tracing of products throughout the supply chain. These technologies help identify where a product has been (track) and where it originated (trace), thus aiding in the identification of potentially counterfeit items (Gianmarco et al., 2015; Li, 2013a).

Figure 3: Examples of traceability technologies (Source: (Li, 2013b))

Several technologies are commonly used for traceability in supply chains, including Radio Frequency Identification (RFID), Electronic Product Codes (EPCs), bar codes, and web portal tools (Agrawal et al., 2010; Li, 2013b; Qian et al., 2011; Ting & Ip, 2013). RFID and EPC systems enable automated data capture and real-time monitoring, enhancing visibility throughout the supply chain. Barcodes remain a cost-effective solution widely adopted in many industries, while web portals provide platforms for accessing and verifying data. These traceability tools enhance supply chain transparency and are essential for detecting and managing counterfeit risks. Figure 3 illustrates some of these technologies used in product tracking and tracing.

1.4 Related Counterfeits Detection Systems

This section surveys the literature to identify existing solutions that prevent and control counterfeit products in the market. Five solutions are discussed: Prooftag solutions, the ConTraffic project, TMDA inspection, the WCO-IPM database, and the pesticide authenticity verification system (Table 1).

Table 1: Strengths and limitations of existing systems (Source: Author)

System	Strengths	Limitations
1. Prooftag Solutions[3]	• Customers use QR codes to prove the authenticity of the products • Professionals use special devices to prove the authenticity of products • Based critically on product package security	Only professionals can validate the authenticity of the high-level product since it requires extra authentication equipment.
2. ConTraffic Project[4]	• Through a traceability mechanism, a carrier website enables users to get status messages of the containers in real-time or in a specified period • Provides an additional source of information on investigations of any counterfeit incident	It lacks information about individual products contained in the containers.
3. TMDA Inspection[5]	Personnel with authorisation can conduct inspections	• Easily interrupted by counterfeiters • Customers and intermediaries are not empowered to detect counterfeits
4. WCO IPM Database[6]	Customs agencies are provided with the appropriate authentication devices to examine all products entering the country	• It is only helpful for internationally shipped goods • Customs agency officers are required to have several different authentication devices (imagine the situation of every product having its authentication device)
5. Pesticides Authenticity Verification System (Ngirwa & Ally, 2018)	• It empowers customers to use mobile apps to identify genuine pesticides • The system records the precise location of a place where counterfeit products have been detected	The system uses batch numbers instead of ID to verify products and thus may readily be interfered with by counterfeiters.

Existing systems have three main strengths: they allow end-users to detect counterfeits by scanning QR or bar codes linked to databases, enable product tracking and tracing along the supply chain, and use physical authentication devices. However, these systems have limitations. They cannot fully prevent counterfeit replication using similar IDs and often exclude key actors like wholesalers, retailers, and consumers from the detection process. This study addresses these gaps by proposing a user-friendly solution that prevents product ID duplication and reuse while ensuring broader stakeholder participation in counterfeit detection across the entire supply chain.

[3] https://prooftag.net/en/home-en/
[4] https://contraffic.jrc.ec.europa.eu/
[5] https://www.tmda.go.tz/
[6] https://www.wcoomd.org/

2 METHODOLOGY

The methodology adopted in this paper is structured into three sections. Section 2.1 details the development of the BLE beacon-based method. In its development, the method integrates with other existing technologies and techniques. Those technologies and techniques include encryption, IoT (beacons), cloud, mobile, and QR codes. On top of those enabler technologies, a technique to safeguard a supply chain of genuine products is devised. That technique also extends to detecting counterfeits attempting to infiltrate a supply chain of genuine products.

After that stage, the next task is transforming the developed method into a computational ambience (section 2.2). That transformation included translating the principles of the proposed method into an executable computer program. The program was then used to test the method. Before testing, settings and the design of experiments were specified. The goal was to ensure that necessary aspects of the testing were considered. That testing was conducted using a medical supply chain in Tanzania.

The central question remains how useful the method is. To answer that question, researchers employed an evaluation technique that involved a survey. Therefore, that survey involved collecting reviews (in section 3.1) from users who participated in testing the method. A questionnaire was used as a tool to collect user reviews. Furthermore, a success evaluation model proposed by (Visser et al., 2013) was adopted to construct a questionnaire (Figure 4).

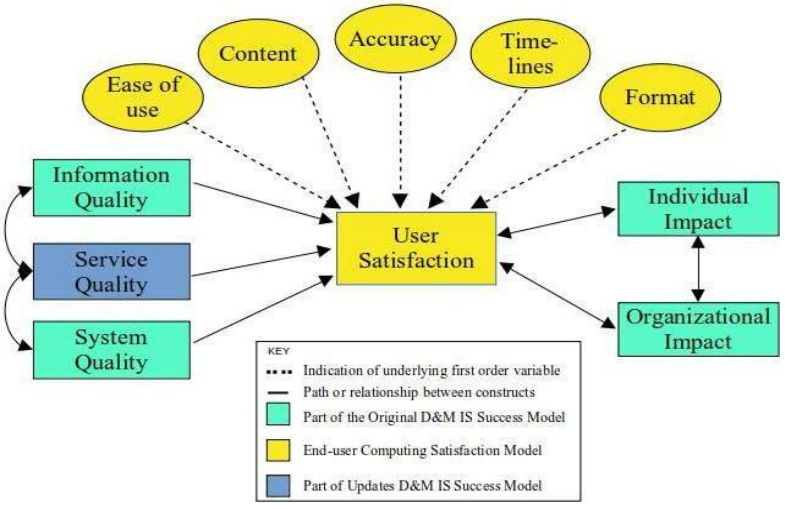

Figure 4: Information system success evaluation model (Source: (Visser et al., 2013)

The evaluation model in Figure 4 comprises the original DeLone and McLean (D&M) Information System (IS) success model, the updated D&M IS success model, and the end-user computing satisfaction model. These models are considered necessary based on their strengths in evaluating information systems. The questionnaire was administered to the respondents after they had been involved in an experiment.

This study involved human participants through a structured survey to evaluate the method's usability and effectiveness. Participants, including supply chain stakeholders and test users, provided written informed consent after a full explanation of the study, with the right to withdraw at any time. No personal data was collected; responses were anonymized and securely stored. Laboratory experiments focused purely on technical performance under controlled conditions. No significant ethical risks were identified due to the study's non-invasive, system-focused nature.

2.1 The Concept of the BLE Beacon-based Method

The method for securing genuine products and detecting infiltration of counterfeit products in supply distinguishes from prior contributions as described next. Nodes in a downstream supply chain, including the manufacturer, are preconfigured in the database by capturing some parameters. This pre-configuration involves recording the GPS location of the physical premises of the nodes involved in the supply chain. Those nodes are manufacturers, wholesalers, sub-wholesalers, and retailers. Manufacturers assign an encrypted, unique ID to each product during the manufacturing process. Multiple products, such as a dozen, may be aggregated to form a single combined package. Afterwards, multiple products constituting a combined package are identified through a group-wise QR code ID attached to a whole package.

Products sold by a manufacturer to a wholesaler are passed to the wholesaler's account, which is linked to that wholesaler's GPS location. This process is referred to in this paper as directing specific products to specific nodes. To make this possible, the manufacturer scans and forwards sold products to a wholesaler's account during the sales process, linking them to pre-configured data (Figure 5). This paper refers to this procedure as "product dispatching."

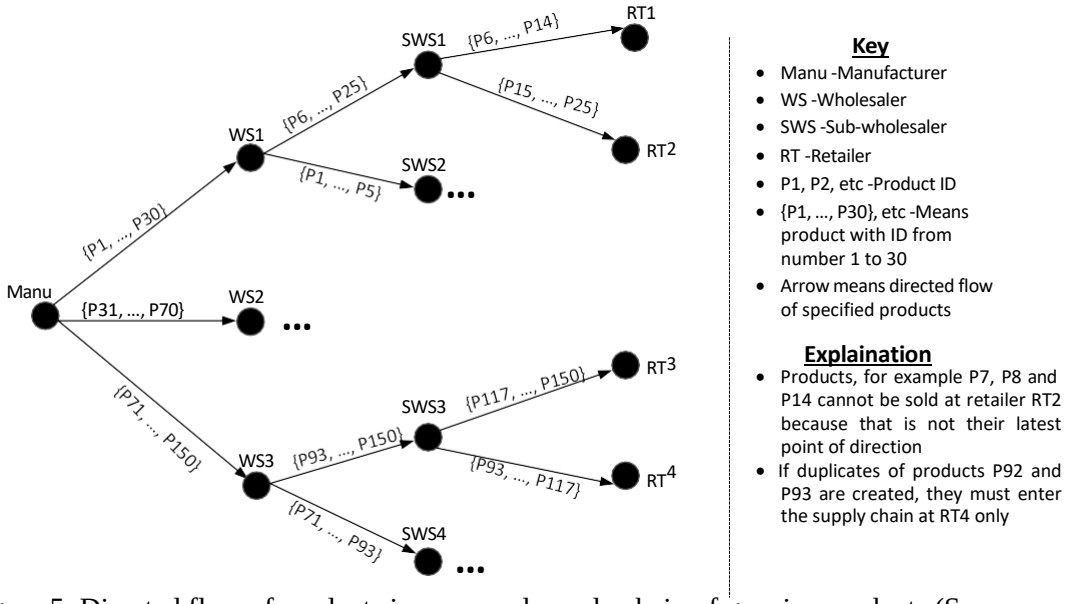

Figure 5: Directed flow of products in a secured supply chain of genuine products (Source: Author)

At his registered facility, the wholesaler uses a QR code reader to scan products he purchased when delivered to his site. The scanning procedure must occur inside a predetermined radius of the wholesaler's premises. Two controls ensure this predefined circumference: the BLE beacon and the geographic location associated with that wholesaler. In this method, this procedure is known as "receiving of products" (Figure 6).

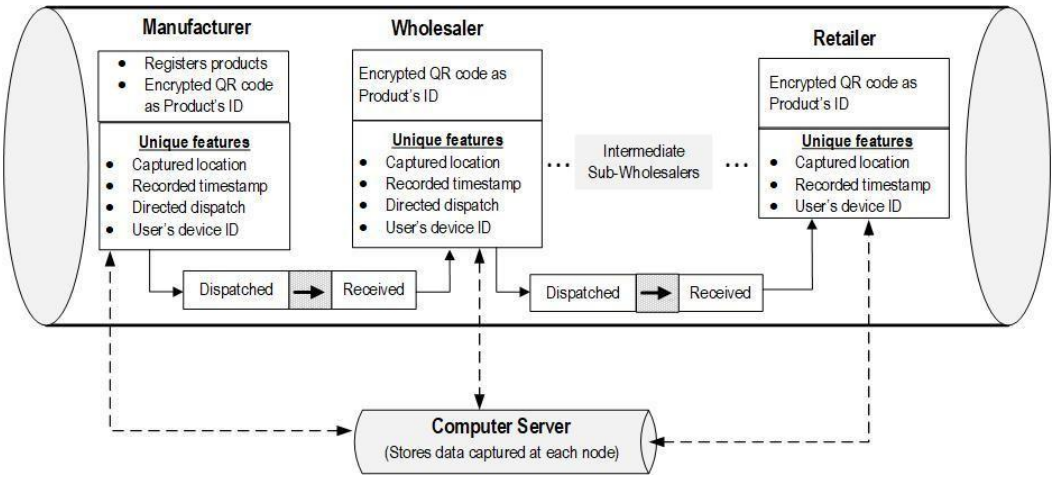

Figure 6: Encrypted QR code and product unique features captured at each node (Source: Author)

In a manner similar to the description in a previous paragraph, when a sub-wholesaler purchases product from a wholesaler or retailer (buyer) purchases products from a wholesaler/sub-wholesaler (seller), the seller must direct those purchased products to a buyer. When the buyer arrives at own premise with those products, QR code of those products must be scanned to signify that products are received. Again, the scanning

process must occur within a predefined circumference of the buyer's premise. Equally, that predefined circumference is ensured using two controls: the BLE beacon and the geographical location affiliated with that buyer (Figure 7). Thus, each site of the wholesaler, sub-wholesaler, and retailer is uniquely identified using the address of the BLE beacon and its geographical location.

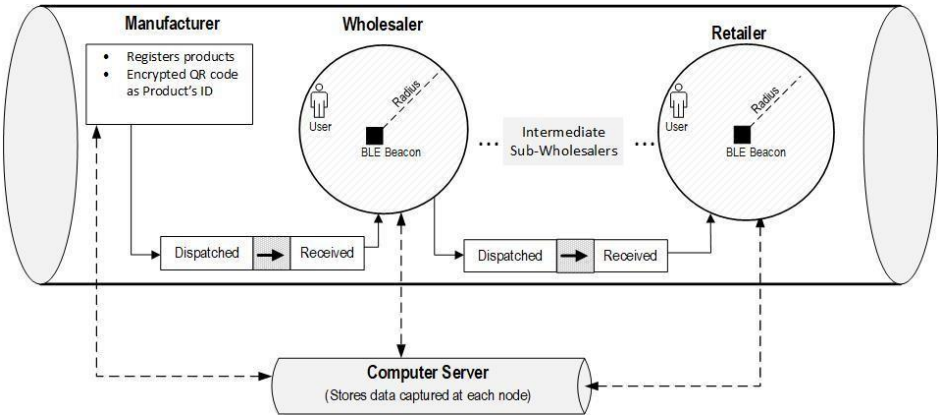

Figure 7: BLE beacons delineating the perimeter of the product scanning area (Source: Author)

Besides offering unique identification, one role of the BLE beacon is to activate the mobile app used to scan products. That mobile app is designed not to work without a BLE beacon. That means scanning a product outside defined circumference of the range of beacon signals will lead into rejection. This range is normally customary set in the BLE beacon. Generally, every product scanning conducted is linked with an address of a BLE beacon as a unique ID of the wholesaler, sub-wholesaler, or retailer at his/her site.

Customers verify whether a product is genuine or counterfeit at the retailer's site. To carry out this verification, customers must download the mobile app from a known server, such as an app store. When customers buy a product within a defined circumference of the retailer’s shop, they use the mobile app to authenticate the product (Figure 8).

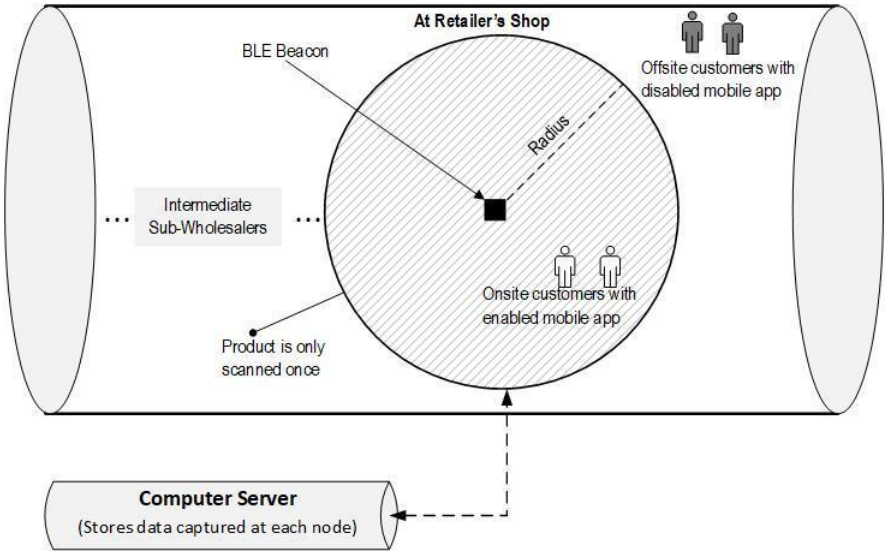

Figure 8: Limiting offsite customers to scan products outside of the retailer's shop (Source: Author)

The mobile app communicates the product's ID, location, and address of the beacon to a web-server for authentication. The algorithm in the server checks whether that product is (i) at a location where it was directed to be, (ii) associated with a unique address of the BLE beacon, (iii) read for the first time at that retailer's store, meaning that it has not been sold before, and; (iv) not expired. If criteria (i) to (iii) are unmet, that product is considered counterfeit. For the last criterion, the customer will be informed that the product has expired. A product scanned at a location where it was not directed to be (latest directed point) will be considered counterfeit even if it is genuine. This is because the movement of products to the downstream supply chain is recorded to ensure that each product remembers its path. This protocol denies an attempt to enter or re-enter a supply chain of registered trademark products. To this end, this protocol forms a basis of the secured supply chain that prevents infiltration of counterfeit products.

Duplicate products that use the ID of the genuine product are prevented from entering the secured supply chain in two ways. First, products are scanned once only and subsequent scans are treated as counterfeits. Second, most mirrored products attempt to enter the supply chain at the latest point of their movement such as a wholesaler's or retailer's premise. Now, if, for example, the retailer engages in counterfeiting, that retailer has two options only. The first option is to sell the counterfeit product and discard the genuine one. The second option is to avoid the counterfeit product and continue to sell the genuine one. As per principles of transaction cost economics,

engaging in the first option is riskier because, in most cases, counterfeit products are relatively sold at a low price compared to genuine ones. If a counterfeiter is not a wholesaler, sub-wholesaler, or retailer, that counterfeiter will need enabling facilities (site, BLE beacon, and location) that must have been reconfigured into a server.

2.2 Implementation of the Method

The present paper refers to implementation as a process of transforming the BLE-based method proposed in section 2.1 into a computer program. That program is a vehicle for proving the method. In this regard, this transformation is specifically set to ascertain the functionality and utility of the established method. Specifying software requirements, designing the system, and coding the method are taken on board. For software requirement specification, the method consists of five main functional requirements:

- *Product registration*: The module allows a manufacturer to generate an encrypted product ID that is attached to a product.
- *Product dispatching*: The module enables a supply chain actor to forward products to the downstream supply chain
- *Receiving products*: The module allows an actor to receive products purchased from the upstream supply chain
- *Product selling:* The retailer hands over a product to the end customer during selling.
- *Authenticating a product:* At this stage, the customer, who must be physically situated within a defined circumference, scans the product's QR code. That process is meant to verify whether a product being purchased is genuine or not.

The method supports five user groups in its implementation: manufacturers, wholesalers, sub-wholesalers, retailers, and end-customers. Coding is achieved using web and mobile application programming technologies and related tools. The method's coding is framed into a control panel and end-user modules. The control panel module is for administration, while the other module serves supply chain actors and end customers.

2.3 Design and Setup of Experiments

The design of this experiment proceeds as follows. The predictors of this experiment are products and actors of the supply chain. The product set is designed to include genuine

and counterfeit products. Small pieces of wood (Figure 9) were used to represent a single unit of a product and small plastic containers were used to aggregate products.

Figure 9: Product sets with their associated QR code (Source: Author)

Figure 10: The iBKS Plus beacon (Source: Author)

Considering that there are many variants of BLE beacons in the market, this study employed the iBKS Plus beacons[7]. Since those beacons can transmit signals up to 100m, each beacon was configured to allow the detection of signals at a preset distance.

The supply chain was designed with five levels of actors: manufacturers, wholesalers, sub-wholesalers, retailers, and end-customers. Beacons are mandatory in facilities owned by wholesalers, sub-wholesalers, and retailers. However, in the present settings, there was also a beacon in the manufacturer's facility (Figure 11).

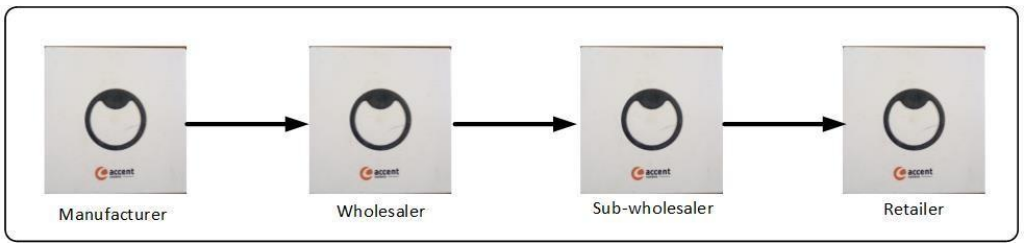

Figure 11:Actors and their associated BLE-beacon devices (Source: Author)

The administrator panel was configured to allow wholesalers, sub-wholesalers, and retailers to operate only within a radius of five (5) meters at their distribution facilities. Then, a distance of seven (7) meters was designed to separate one distribution facility from another—the distance aimed at avoiding signal interferences that can emerge

[7] https://accent-systems.com/product/ibks-plus/

among BLE beacons and GPS services. Further, the proposed method required a researcher to identify and configure the GPS coordinates of all involved distribution facilities, excluding the manufacturer.

Regarding outcomes, a prototype of the method was expected to respond depending on how predictors meet the criteria established. Expectedly, the outcome would be that a product is genuine, counterfeit, expired, invalid BLE-beacon used, or no response available.

The experiment used the following settings. The product sets were of three categories: single aggregation set, double aggregation set, and triple aggregation set. The single aggregation set was generated with five (5) units of genuine products, which were directed from a manufacturer's downstream supply chain. Then, purposely at the retailer's distribution facility, two (2) products of genuine products were set to be replaced with counterfeit ones. This setting aimed to demonstrate how the proposed method can detect and prevent the infiltration of counterfeit products. Table 2 presents the experimental setup of this category whereas:

- One (1) represents genuine,
- Zero (0) represents not genuine (including counterfeit, expired, not available),
- A tick (✓) represents that an actor has permission to do such task, and;
- A cross sign (✕) represents that an actor is not permitted to carry out such a task.

Table 2: A single aggregation of products (Source: Author)

Actor	Single Aggregation Set (Set A)					Action		
	A_1	A_2	A_3	A_4	A_5	Receive	Direct	Buy
Manufacturer	1	1	1	1	1	✕	✓	✕
Wholesaler	1	1	1	1	1	✓	✓	✕
Sub-wholesaler	1	1	1	1	1	✓	✓	✕
Retailer	1	0	1	0	1	✓	✕	✕
End-customer	1	0	1	0	1	✕	✕	✓

The double aggregation set (Table 3) was generated with two subsets, each containing three (3) units of genuine products. This aggregation set was required to be directed from a manufacturer's distribution facility downstream supply chain to the retailer's distribution facility. Then, purposely at the wholesaler's distribution facility, one (1) of

the two subsets is set to be replaced with the counterfeit set. At this point (wholesaler's distribution facility), any set of counterfeit products is not expected to be directed to the downstream distribution facilities, including sub-wholesalers and retailers. These settings were also available to demonstrate how the proposed method detects and prevents unlawful infiltration.

Table 3: A double aggregation set of products (Source: Author)

Actor	Double Aggregation Set (Set B)						Action		
	B1			B2			Receive	Direct	Buy
	B11	B12	B13	B21	B22	B23			
Manufacturer	1	1	1	1	1	1	×	✓	×
Wholesaler	1	1	1	0	0	0	✓	✓	×
Sub-wholesaler	1	1	1	-	-	-	✓	✓	×
Retailer	-	-	-	-	-	-	✓	×	×
End-customer	-	-	-	-	-	-	×	×	✓

Further, in the double aggregation set, a retailer was set to use a BLE beacon not associated with his distribution facility. Similarly, the computer server was designed to handle signals from BLE beacons that have already been set up and are limited to a single location. This setting aimed to reveal how the proposed method can capture any activity involved with an invalid use of BLE beacons.

Finally, a triple aggregation set (Table 4) was generated with two (2) outer subsets of genuine products, each subset holding the other two (2) inner subsets. Afterwards, two (2) units of genuine products were inserted in every inner subset of genuine products.

Table 4: A triple aggregation set of products (Source: Author)

Actor	Triple Aggregation Set (Set C)								Action		
	C1				C2						
	C11		C12		C21		C22				
	C111	C112	C121	C122	C211	C212	C221	C222	**Receive**	**Direct**	**Buy**
Manufacturer	1	1	1	1	1	1	1	1	×	✓	×
Wholesaler	1	1	1	1	1	1	1	1	✓	✓	×
Sub-wholesaler	1	1	1	1	-	-	-	-	✓	✓	×
Retailer	1	1	-	-	-	-	-	-	✓	×	×
End-customer	1	-	-	-	-	-	-	-	×	×	✓

With the triple aggregation set, one of the two outer subsets of genuine products was set to be currently received and available only at the wholesaler's distribution facility. The remaining outer subset of genuine products was set to be available at the sub-wholesaler's distribution facility for being directed to the downstream nodes. A retailer was placed to receive genuine products (two units) from the sub-wholesaler's

distribution facility; afterwards, the end customer can now buy one unit of genuine product from the retailer's distribution facility. The triple aggregation set was essential for finding how the proposed method can manage distributions of genuine product sets across various supply chain actors.

All actors in the supply chain must install the mobile app from the provided source. According to the already established setups, the actor for the manufacturer's distribution facility generated the product aggregation sets (Figure 12).

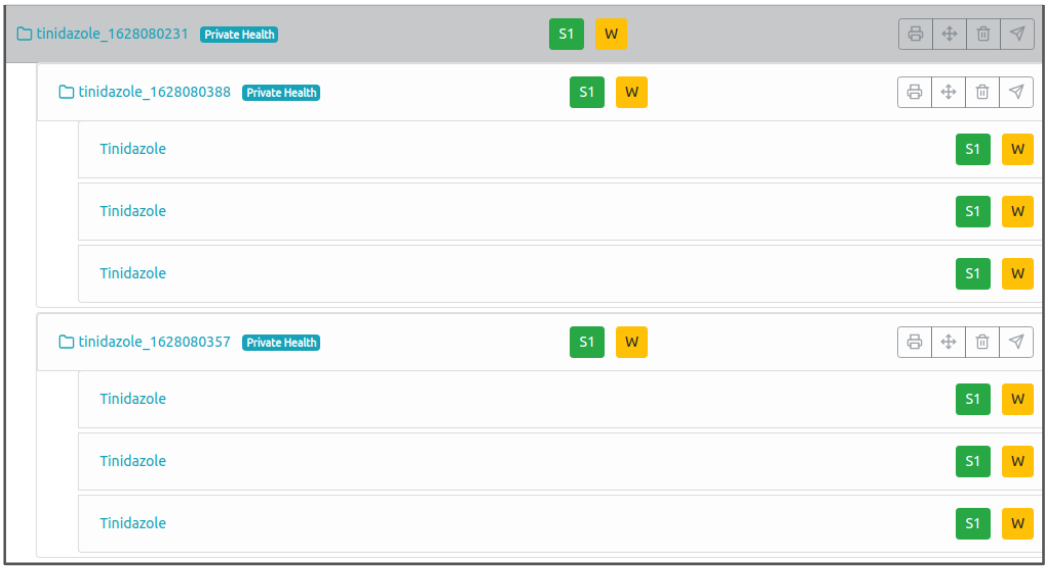

Figure 12: A web view of double aggregation at the manufacturer's facility (Source: Author)

Afterwards, as per design, the respective QR codes were printed accordingly into their product packages (see Figure 9). The remaining actors, representing wholesalers, sub-wholesalers, retailers, and end-customers, scanned the QR codes of the relevant product and got the responses accordingly (Figure 13).

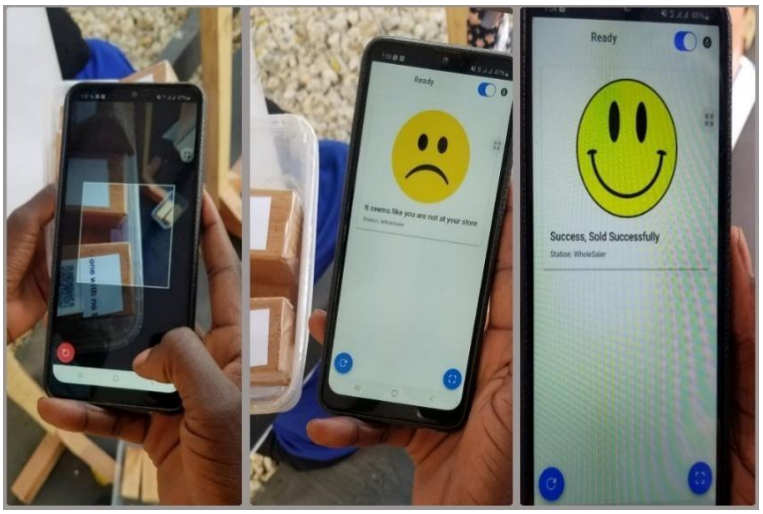

Figure 13: The snapshots of the mobile app scan responses during an experiment (Source: Author)

The mobile application powered the scanning of a QR code and required permission to access the GPS and Bluetooth services. Accordingly, a relevant player's smartphone was required to have internet access so that the mobile app could communicate with its back-end programs.

3 RESULTS

This section presents the results of two key evaluation activities. First, it presents a user review survey assessing system effectiveness, usability, and overall value (subsection 3.1). Secondly, it presents experimental testing of the method used to simulate product flows and counterfeiting scenarios (subsection 3.2).

3.1 Evaluation through User Survey

A total of 38 participants participated in the user evaluation: 57.5% from Mzumbe University and 42.5% from medical facilities. Among university respondents, ICT students made up 56.5%, while 43.5% were from other programs. Among medical personnel, the majority were pharmacists (58%).

Participants evaluated six constructs based on system quality, usability, usefulness, and impact (Table 5).

Table 5: Evaluation results for the close-ended section of the questionnaire (Source: Author)

Success evaluation construct	Item evaluated	Results
Service quality	Response time	• 50% below 5 seconds • 50% response time was between 5 to 10 seconds
Information quality	Usefulness (output and data	• 62.5% high quality

Success evaluation construct	Item evaluated	Results
	quality)	• 37.5% moderate quality
End-user computing satisfaction	Ease of use, content, and format	• 43% required moderate guidance • 30% required low guidance • 22.5% required high guidance
Organisational impact	The overall impact on all actors	• 52.5% said it has a higher impact • 47.5% moderate
System quality	Ease of access and ease of functioning	• 55% required no guidance • 32.5% required low guidance • 7.5% required moderate guidance • 5% required high guidance
Individual impact	Usability	• 75% high • 25% moderate

Table 5 presents the results from the close-ended questionnaire across six evaluation constructs. For service quality, 50% of respondents experienced response times below 5 seconds, and 50% between 5–10 seconds. Information quality was rated high by 62.5% and moderate by 37.5%. In end-user computing satisfaction, 30% needed little guidance, 43% moderate, and 22.5% high. Organisational impact was rated high by 52.5% and moderate by 47.5%. System quality results showed 55% required no guidance and 32.5% low guidance. For individual impact, 75% of respondents expressed willingness to use the system in daily routines, and 25% showed moderate willingness.

Open-ended responses further validated these observations (Table 4). Most notably, 67.5% recommended immediate deployment of the method, while 30% emphasized the need for support for non-smartphone users.

Table 6: Evaluation results for the open-ended section of the questionnaire (Source: Author)

Feedback from participants	Improvements suggested by participants
Deploy it immediately (67.5%)	Use local language (7.5%)
Use without Bluetooth (2.5%)	Add payment facilities (10%)
What about the affordability of the beacon devices? (5%)	Consider non-smartphone users (30%)
Access a service anywhere, not only in the actor's distribution facility (2.5%)	Improve the quality of QR codes (10%)
Impose purchase discounts (2.5%)	Not only medicines, include other products (2.5%)
Education and training to expected users (2.5%)	Add more details about a medicine (20%)

Other suggestions included enhancing QR code quality, using local languages, and integrating more detailed product information. Concerns about BLE beacon affordability were also raised, though the beacon's relatively low cost mitigated this.

3.2 Experimental Results from Simulated Supply Chain

Experimental results were obtained from controlled simulations using three product aggregation setups: single, double, and triple aggregation. In the single aggregation setup, five genuine products were distributed, and two (A_2 and A_4) were intentionally replaced with counterfeit ones at the retail level. These changes and resulting system outputs were recorded in Table 7.

Table 7: The results for a single aggregation set (Source: Author)

Actors	**SINGLE AGGREGATION (SET A)**				**Results**		
	A1	**A2**	**A3**	**A4**	**Expected**	**Observed**	**Remarks**
M	1	1	1	1	-	-	-
W	1	1	1	1	-	-	-
S	1	1	1	1	-	-	-
R	1	0	1	0	-	-	-
E	1	0	1	0	Counterfeit (A_2, A_4)	Counterfeit (A_2, A_4)	Pass

In the double aggregation setup, one subset of genuine products (B_2) was replaced with counterfeits at the wholesaler's facility. When directed further to a sub-wholesaler, the system successfully flagged B_2 as counterfeit. Additionally, an attempt to scan using an invalid BLE beacon was rejected. The recorded results are shown in Table 8.

Table 8: The results for the double aggregation set (Source: Author)

	Double Aggregation (Set B)						Results		
		B1			B2		Expected	Observed	Remarks
Actors	B11	B12	B13	B21	B22	B23			
M	1	1	1	1	1	1	-	-	-
W	1	1	1	0	0	0	Counterfeit (B_2)	Counterfeit (B_2)	Pass
S	1	1	1	-	-	-	-	-	-
R	-	-	-	-	-	-	Invalid beacon	Invalid beacon	Pass
E	-	-	-	-	-	-	-	-	-

For the triple aggregation setup, genuine products were distributed across multiple levels, with subset C_2 made available only at the wholesaler's facility. Scanning attempts by actors outside that scope—such as sub-wholesalers, retailers, or customers—were denied. Table 9 presents the outcomes of this setup.

Table 9: The results for the triple aggregation set (Source: Author)

	Triple Aggregation (Set C)								Results		
	C1				C2						
	C11		C12		C21		C22		Expected	Observed	Remarks
Actors	**C111**	**C112**	**C121**	**C122**	**C211**	**C212**	**C221**	**C222**			
M	1	1	1	1	1	1	1	1	-	-	-
W	1	1	1	1	1	1	1	1	Available (C2)	Available (C2)	Pass
S	1	1	1	1	-	-	-	-	Available (C12)	Available (C12)	Pass
R	1	1	-	-	-	-	-	-	Available (C112)	Available (C112)	Pass
E	1	-	-	-	-	-	-	-	Available (C111)	Available (C111)	Pass

The experimental procedures were complemented by a user evaluation survey involving 38 participants. Respondents included university students and healthcare professionals. Data was collected through a structured questionnaire, combining six close-ended evaluation constructs (Table 5) and open-ended questions (Table 4). Responses were analysed to generate frequencies and capture user feedback related to the proposed detection method.

4 DISCUSSION

The primary objective of this study was to develop a method for securing genuine products in supply chains and detecting counterfeit infiltration using Bluetooth Low Energy (BLE) beacons. The evaluation of this method, based on experimental tests and user surveys, confirms its technical validity and practical applicability in real-world settings. This discussion integrates quantitative and qualitative results, reflecting on their implications while situating the method within the broader landscape of counterfeit prevention technologies. The discussion comprises user evaluation (subsection 4.1) and contributions and distinctiveness (subsection 4.2), which reflect the experimental results. The section ends by providing a contribution to practice and theory in subsection 4.3.

4.1 User Evaluation

The discussion on user evaluation, among others, focuses on system performance and responsiveness, detection accuracy, user experience, usefulness and societal impact.

***Performance and system responsiveness*.** The evaluation of service quality demonstrated that the BLE beacon-based method is responsive, with 50% of users receiving system responses in under five seconds and the other half within 5–10

seconds. This level of performance affirms the method's viability for real-time use. However, it is worth noting that response time may be influenced by external factors such as internet speed and QR code print quality—an area for further optimization.

***Detection accuracy and system control*.** From the experiments, the method accurately detected counterfeit products introduced at different points in the supply chain. In the single-aggregation setup, counterfeit products injected at the retail level were correctly flagged and reported at the customer level. In the double aggregation experiment, the system successfully identified a counterfeit subset introduced at the wholesaler level. The triple aggregation case further confirmed that products could only be verified at the distribution point where they were supposed to be available; any scanning attempts outside the assigned zones were automatically rejected.

These findings demonstrate the effectiveness of location-aware verification and BLE-beacon control mechanisms in safeguarding the movement of genuine products. Attempts to use unregistered beacons or scan products outside defined distribution zones were blocked, reinforcing the system's ability to secure the supply chain from unauthorised or counterfeit activity. Additionally, the method rejected QR codes not generated by the system and denied repeat scans, thereby preventing duplication or reuse of product IDs—a limitation commonly found in many existing solutions.

User experience and adoption readiness. The construct of end-user computing satisfaction revealed that 30% of users required little guidance, 43% required moderate, and 22.5% required high guidance when using the system for the first time. This suggests that the method is generally user-friendly but may benefit from minor usability enhancements or brief training modules to increase confidence in first-time users. Once familiar with the system, 55% of users reported that they would not need any guidance in subsequent use, while 32.5% would need minimal help—an encouraging indicator of ease of adoption.

Perceived usefulness and usability. Respondents rated information quality highly, with 62.5% confirming the system's usefulness in detecting counterfeits. Similarly, individual impact results showed that 75% of users would integrate the system into their daily routines if made publicly available. This level of endorsement reflects the method's practical relevance, especially in contexts where users—such as pharmacists, clinicians, and students—frequently engage in verifying product authenticity.

Organizational and societal impact. The method was also found to have a strong organizational impact, with over 52.5% of respondents acknowledging its capacity to prevent counterfeits and enhance traceability across all actors. The fact that each product can "remember" its path downstream—due to its association with a unique QR code and BLE beacon—provides a robust record of transaction history, a feature lacking in many existing solutions.

In terms of societal readiness, 67.5% of participants recommended immediate deployment of the method, underscoring the urgency of implementing practical solutions to the problem of counterfeiting, especially in markets like Tanzania. However, some limitations were also highlighted.

4.2 Contributions and Distinctiveness

This study presents a novel method for securing supply chains against counterfeit products by integrating Bluetooth Low Energy (BLE) beacons with encrypted product identification and location-based controls. Unlike traditional approaches focused mainly on manufacturers or customs, this method involves all key actors—manufacturers, wholesalers, sub-wholesalers, retailers, and end customers—ensuring verification at every transaction point. A standout feature is its geofencing capability: BLE beacons placed at designated distribution points limit product authentication to specific physical areas, rejecting scans made outside authorized zones. This prevents common vulnerabilities in QR- and RFID-based systems, such as ID reuse or package tampering. Additionally, each product carries a unique encrypted ID from manufacturing and maintains a "transactional memory," enabling the system to detect when a product is scanned multiple times, at the wrong location, or with an unauthorized QR code—flagging it as counterfeit and enhancing traceability across the supply chain.

The method also empowers end-users by enabling product verification via a mobile app, promoting consumer trust and making authentication accessible beyond professionals with specialized tools. This democratized approach not only improves transparency but also creates a final layer of defense against counterfeit infiltration. Technically lightweight and cost-effective, the solution eliminates the need for costly infrastructure like RFID gates, relying instead on affordable BLE beacons and smartphones. Its scalability and suitability for low-resource settings make it a practical tool for combating counterfeit goods in diverse markets. Backed by positive user evaluations, the proposed method

offers a comprehensive, inclusive, and economically viable approach to safeguarding supply chains—especially in developing regions where such solutions are most needed.

4.3 Contribution to Practice and Theory

From a practical perspective, the method offers a ready-to-deploy prototype that addresses real-world supply chain threats with minimal technical complexity. It promotes decentralized counterfeit detection, supports policy implementation through traceable product flows, and can be adapted across industries vulnerable to counterfeiting, such as pharmaceuticals, electronics, and cosmetics. Theoretically, the study contributes to the growing body of literature on supply chain security and anti-counterfeit technology by introducing a hybrid model that blends traceability, location-aware verification, and actor-specific authentication. It also validates the role of lightweight, accessible technologies—such as BLE beacons—in establishing secure, inclusive digital supply chain infrastructures.

5 CONCLUSION

Counterfeit detection and prevention remains a global concern, affecting consumers, manufacturers, and supply chain stakeholders. Despite ongoing efforts by industry and academia, existing solutions often fall short, particularly in preventing the duplication of product identifiers and in engaging a broad range of actors. Many current approaches focus narrowly on manufacturers or customs authorities, leaving gaps in downstream verification. This paper presents a novel method designed to protect supply chains of genuine products by involving all key stakeholders—manufacturers, wholesalers, sub-wholesalers, retailers, and end consumers—in both the safeguarding and detection process.

The method begins by registering each product at the point of manufacture and tracking it throughout its journey using BLE beacons, GPS, and other control parameters. These technologies create a directed flow of products, enabling verification at each supply chain node. The method ensures that every actor plays a role in tracing product history, which enhances transparency, increases trust, and enables early detection of counterfeit infiltration.

Despite these contributions, future work is essential. The current method has only been validated in controlled laboratory settings. Field testing will help evaluate its real-world

effectiveness. Additionally, because it relies on smartphones with internet access, making the system accessible via basic mobile phones could significantly improve its affordability and reach in low-resource settings.

REFERENCES

Agnusdei, G. P., Coluccia, B., Elia, V., & Miglietta, P. P. (2022). IoT technologies for wine supply chain traceability: Potential application in the Southern Apulia Region (Italy). *Procedia Computer Science*, *200*(2019), 1125–1134. https://doi.org/10.1016/j.procs.2022.01.312

Agrawal, Y., Shah, R., & Prajapati, P. (2010). Anticounterfeit packaging technologies. *Journal of Advanced Pharmaceutical Technology & Research*, *1*(4), 368. https://doi.org/10.4103/0110-5558.76434

Altaf, F., Prateek, K., & Maity, S. (2022). Beacon Non-Transmission attack and its detection in intelligent transportation systems. *Internet of Things*, *20*(October), 100602. https://doi.org/10.1016/j.iot.2022.100602

Amit, Y., Felzenszwalb, P., & Girshick, R. (2020). Object Detection. In *Computer Vision* (pp. 1–9). Springer International Publishing. https://doi.org/10.1007/978-3-030-03243-2_660-1

Andreev, P. I., & Aprahamian, B. R. (2018). Analytical comparison of bluetooth low energy beacons. *2018 20th International Symposium on Electrical Apparatus and Technologies, SIELA 2018 - Proceedings*, 1–4. https://doi.org/10.1109/SIELA.2018.8447078

Anilkumar, P. S., Yagneshkumar, S. R., & Bharatkumar, T. R. (2012). *Anticounterfeit Packaging Foil* (WO2012131704A3). European Patent Register.

Asadizanjani, N., Rahman, M. T., & Tehranipoor, M. (2021). *Physical Assurance for Electronic Devices and Systems*. Springer International Publishing. https://doi.org/10.1007/978-3-030-62609-9

Bansal, D., Malla, S., Gudala, K., & Tiwari, P. (2013). Anti-Counterfeit Technologies: A Pharmaceutical Industry Perspective. *Scientia Pharmaceutica*, *81*(1), 1–13. https://doi.org/10.3797/scipharm.1202-03

Bian, X., & Moutinho, L. (2009). An investigation of determinants of counterfeit purchase consideration. *Journal of Business Research*, *62*(3), 368–378. https://doi.org/10.1016/j.jbusres.2008.05.012

Canayaz, M., & Gurun, U. G. (2018). The Real Effects of Fake Goods: Counterfeit Products and Firm Value. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3231962

Citti, C., Braghiroli, D., Vandelli, M. A., & Cannazza, G. (2018). Pharmaceutical and biomedical analysis of cannabinoids: A critical review. *Journal of Pharmaceutical and Biomedical Analysis*, *147*(1), 565–579. https://doi.org/10.1016/j.jpba.2017.06.003

Commuri, S. (2009). The Impact of Counterfeiting on Genuine-Item Consumers' Brand Relationships. *Journal of Marketing*, *73*(3), 86–98. https://doi.org/10.1509/jmkg.73.3.86

Correa, M., Hermosilla, G., Verschae, R., & Ruiz-Del-Solar, J. (2012). Human detection and identification by robots using thermal and visual information in domestic environments. *Journal of Intelligent and Robotic Systems: Theory and Applications*, *66*(1–2), 223–243. https://doi.org/10.1007/s10846-011-9612-2

Cruikshank, L. (2014). *How Anti-Counterfeit Innovations Can Improve Global Healthcare Supply Chains*. https://www.innovationsinhealthcare.org/document/how-anti-counterfeit-innovations-can-improve-global-healthcare-supply-chains-(2014)/

Davison, M. (2011). *Pharmaceutical Anti-Counterfeiting: Combating the Real Danger from Fake Drugs*. Wiley & Sons, Inc.

Deloitte. (2015). *Strategic Review of the Medical Stores Department of Tanzania: The Journey to Efficiency - Final Report*. https://hssrc.tamisemi.go.tz/storage/app/uploads/public/5ad/0cc/69c/5ad0cc69c477c212179396.pdf

El-Dahiyat, F., Fahelelbom, K. M. S., Jairoun, A. A., & Al-Hemyari, S. S. (2021). Combatting Substandard and Falsified Medicines: Public Awareness and Identification of Counterfeit Medications. *Frontiers in Public Health*, *9*(October), 1–8. https://doi.org/10.3389/fpubh.2021.754279

Electronicsforu. (2016). *Bluetooth Beacon Applications and Real World Developer Issues*. https://iot.electronicsforu.com/expert-opinion/bluetooth-beacon/

Felzenszwalb, P. F., Girshick, R. B., & McAllester, D. (2010). Cascade object detection with deformable part models. *2010 IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, *56*(9), 2241–2248. https://doi.org/10.1109/CVPR.2010.5539906

Filippoupolitis, A., Oliff, W., Takand, B., & Loukas, G. (2017). Location-Enhanced Activity Recognition in Indoor Environments Using Off the Shelf Smart Watch Technology and BLE Beacons. *Sensors*, *17*(6), 1230. https://doi.org/10.3390/s17061230

Ghadge, A., Duck, A., Er, M., & Caldwell, N. (2021). Deceptive counterfeit risk in global supply chains. *Supply Chain Forum*, *22*(2), 87–99. https://doi.org/10.1080/16258312.2021.1908844

Gianmarco, B., Enrico, C., Aris, T., Igor, N. F., & Riccardo, S. (2015). *Survey of techniques for the fight against counterfeit goods and Intellectual Property Rights (IPR) infringement* (Vol. 151, Issue 1). https://doi.org/https://doi.org/10.2788/97231

Gonzalez, A., Gonzalez, A., & Sabarez, A. (2014). *Method, apparatus and system for crowd sourced counterfeit detection and brand assurance* (US20140252080).

Jeon, K. E., She, J., Soonsawad, P., & Ng, P. C. (2018). BLE Beacons for Internet of Things Applications: Survey, Challenges, and Opportunities. *IEEE Internet of Things Journal*, *5*(2), 811–828. https://doi.org/10.1109/JIOT.2017.2788449

Kros, J. F., Liao, Y., Kirchoff, J. F., & Zemanek Jr., J. E. (2019). Traceability in the Supply Chain. *International Journal of Applied Logistics*, *9*(1), 1–22. https://doi.org/10.4018/IJAL.2019010101

Le Roux, A., Bobrie, F., & Thébault, M. (2016). A typology of brand counterfeiting and imitation based on a semiotic approach. *Journal of Business Research*, *69*(1), 349–356. https://doi.org/10.1016/j.jbusres.2015.08.007

Li, L. (2012). Effects of Enterprise Technology on Supply Chain Collaboration and Performance. In *Enterprise Information Systems* (Vol. 6, Issue 1, pp. 201–210). https://doi.org/10.1007/978-3-642-28827-2_14

Li, L. (2013a). Technology designed to combat fakes in the global supply chain. *Business Horizons*, *56*(2), 167–177. https://doi.org/10.1016/j.bushor.2012.11.010

Li, L. (2013b). Technology designed to combat fakes in the global supply chain. *Business Horizons*, *56*(2), 167–177. https://doi.org/10.1016/j.bushor.2012.11.010

Lin, S., Shi, Q., & Zhou, N. (2022). Construction of a Traceability System for Food Industry Chain Safety Information Based on Internet of Things Technology. *Frontiers in Public Health*, *10*(May), 1–14. https://doi.org/10.3389/fpubh.2022.857039

Manasreh, D., Swaleh, S., & Nazzal, M. D. (2023). Evaluation of BLE beacon technology for time critical I2V communication to support CAV deployment on urban roadways. *Internet of Things (Netherlands)*, *24*(September), 100932. https://doi.org/10.1016/j.iot.2023.100932

Ngirwa, C. C., & Ally, M. (2018). An ICT Based Solution for Pesticides Authenticity Verification: A Case of Tanzania. *Journal of Information Systems Engineering & Management*, *3*(4). https://doi.org/10.20897/jisem/3938

Park, I.-Y., Ahn, S., Kim, Y., Bae, H.-S., Kang, H.-S., Yoo, J., & Noh, J. (2017). Serial number coding and decoding by laser interference direct patterning on the original product surface for anti-counterfeiting. *Optics Express*, *25*(13), 14644. https://doi.org/10.1364/oe.25.014644

Plane, D., & Chen, G. (2016). Trade in Counterfeit and Pirated Goods. In *Simone Intellectual Property Services (SIPS)*. OECD. https://doi.org/10.1787/9789264252653-en

Qian, Y., Jin, B., & Fang, W. (2011). Heuristic algorithms for effective broker deployment. *Information Technology and Management*, *12*(2), 55–66. https://doi.org/10.1007/s10799-011-0095-4

Sterling, B. G., Polonetsky, J., & Fan, S. (2014). *BEACONS* (Issue December, pp. 1–8).

Ting, S. L., & Ip, W. H. (2013). Combating the counterfeits with web portal technology. *Enterprise Information Systems*, *9*(7), 661–680. https://doi.org/10.1080/17517575.2012.755713

TMDA. (2021). *Home Page*. https://www.tmda.go.tz/

USAID. (2016). *Health Logistics in Tanzania*. https://pdf.usaid.gov/pdf_docs/PA00MFMD.pdf

Verschae, R., & Ruiz-del-Solar, J. (2015). Object Detection: Current and Future Directions. *Frontiers in Robotics and AI*, *2*. https://doi.org/10.3389/frobt.2015.00029

Visser, M., Van Biljon, J., & Herselman, M. (2013). Evaluation of management information systems: A study at a further education and training college. *SA Journal of Information Management*, *15*(1), 1–8. https://doi.org/10.4102/sajim.v15i1.531

Warrier, J. W. C. M. A. M. Y. H. A. Q. A. (2020). Reaching the Last Mile : Tanzania ' s Medical Supply Chain. In *Reach Project*. https://reachalliance.org/case-study/reaching-the-last-mile-tanzanias-medical-supply-chain/#:~:text=Tanzania has gradually and purposefully,platforms more precise and efficient.

Wilson, J. M., Grammich, C., & Chan, F. (2016). Organizing for brand protection and responding to product counterfeit risk: An analysis of global firms. *Journal of Brand Management*, *23*(3), 345–361. https://doi.org/10.1057/bm.2016.12

Wu, H., & Tsai, C. (2018). A home security system for seniors based on the beacon technology. *Concurrency and Computation: Practice and Experience*, *30*(15). https://doi.org/10.1002/cpe.4496

Yuanli, C., Yonghui, H., Li, L., Yongbing, Q., Miaofeng, X., & Weidong, Z. (2017). *Quantitative detection method of bovine-derived and porcine- derived components based on droplet digital pcr (polymerase chain reaction) as well as primer, probe and kit* (CN106676189A). European Patent Register.

Zhao, G., Zhao, H., & Yu, D. (2018). *An anti-counterfeit label and a method for detecting and authenticating the genuine product of a registered trademark thereof* (CN108985431). WIPO.

Zhao, G., Zhao, H., & Yu, D. (2019). *Anti-counterfeiting label and method for detecting and authenticating authenticity of commodity of registered trademark by using same* (PCT/CN2018/107033). WIPO. https://patentscope.wipo.int/search/en/detail.jsf?docId=WO2019072082&tab=PCTBIBLIO