electronics

Article

Fog-Computing-Based Cyber–Physical System for Secure Food Traceability through the Twofish Algorithm

Kamran Ahmad Awan [1], Ikram Ud Din [1,*], Ahmad Almogren [2] and Byung-Seo Kim [3,*]

[1] Department of Information Technology, The University of Haripur, Haripur 22620, Pakistan; kamranawan.2955@gmail.com
[2] Department of Computer Science, College of Computer and Information Sciences, King Saud University, Riyadh 11633, Saudi Arabia; ahalmogren@ksu.edu.sa
[3] Department of Software and Communication Engineering, Hongik University, Sejong 30016, Korea
* Correspondence: ikramuddin205@yahoo.com (I.U.D.); jsnbs@hongik.ac.kr (B.-S.K.)

Abstract: The Internet is an essential part of daily life with the expansion of businesses for maximizing profits. This technology has intensely altered the traditional shopping style in online shopping. Convenience, quick price comparison, saving traveling time, and avoiding crowds are the reasons behind the abrupt adoption of online shopping. However, in many situations, the product provided does not meet the quality, which is the primary concern of every customer. To ensure quality product provision, the whole food supply chain should be examined and managed properly. In food traceability systems, sensors are used to gather product information, which is forwarded to fog computing. However, the product information forwarded by the sensors may not be similar, as it can be modified by intruders/hackers. Moreover, consumers are interested in the product location, as well as its status, i.e., manufacturing date, expiry date, etc. Therefore, in this paper, data and account security techniques were introduced to efficiently secure product information through the Twofish algorithm and dual attestation for account verification. To improve the overall working, the proposed mechanism integrates fog computing with novel modules to efficiently monitor the product, along with increasing the efficiency of the whole working process. To validate the performance of the proposed system, a comparative simulation was performed with existing approaches in which Twofish showed notably better results in terms of encryption time, computational cost, and the identification of modification attacks.

Keywords: fog computing; cyber–physical system; food traceability; block encryption; food security; food processing; fog computing; food security; modification attack

Citation: Awan, K.A.; Din, I.U.; Almogren, A.; Kim, B.-S. Fog-Computing-Based Cyber–Physical System for Secure Food Traceability through the Twofish Algorithm. *Electronics* **2022**, *11*, 283. https://doi.org/10.3390/electronics11020283

Academic Editor: Amir Mosavi

Received: 26 November 2021
Accepted: 12 January 2022
Published: 17 January 2022

1. Introduction

Since the last decade, quality products have spread throughout the world. Customers can buy quality product items from different resources using devices, such as mobile phones, laptops, notebooks, personal computers, smart wristwatches, and so on [1]. Due to several distinct distribution channels, the traceability of each product raises challenges for maintaining the integrity of product information sensed at the sensor layer and supply chain information collected by the monitoring layer. In food traceability systems, product information is gathered with the help of different sensors [2], whereas sensors are located at different stages of the supply chain such as farming, food processing, food packing, food storage, distribution, retailers, etc. Therefore, sensors are responsible for obtaining product information from different stages and forwarding it to fog computing [3]. In food traceability, it is important to identify the actual content and information of the food product because it is essential to find the ingredients and product values used in various food products [4]. Due to the mentioned challenges, food traceability plays an important role in the food supply chain domain [5]. The robustness of traceability is important because a weak system may cause a negative impression for the customers. If the negative

impression increases, then the customers may not rely on any manufacturing platform of food items [6]. Traceability is a major challenge in the management of the food supply chain, which is the process of monitoring the food supply chain and tracking food products in a dependable and accurate form [7]. Further, the formation of a secure, efficient, and reliable food traceability system is a significant resolution to the supply chain. Such a secure food traceability system increases production, the market value of the product, and consumers' satisfaction and trust [8,9]. In the food supply chain, food products pass through different phases, and it is important to trace every phase of the product. Since food products are developed according to consumers' needs, the food traceability system must be accountable for forwarding accurate product information to fog computing [10].

With the rapid growth of information technology, products' quality maintenance is the major issue [11]. Due to this, consumers are interested in buying better-quality items. There are still some issues, when the system obtains product information and wants to share it with fog computing; for example, an intruder may interrupt and change the actual product information [12]. In such a case, the system may forward the wrong information to fog computing, which has a negative impression on the supply chain and product quality on the market. The food product is traced from the initial phase of farming to retailers. Before this channel, various stages are involved in the food supply chain [13]. It is necessary to trace the food product in every phase, and correct product information should be forwarded. It is the responsibility of the system to provide correct information throughout the supply chain during its production process. The proposed approach (FogAuth-FT) provides the capability to maintain adequate security, which will provide reliable product information and remove the poor-quality products from the supply chain. Moreover, it should increase the consumers' trust level regarding the product and supply chain of manufacturers. To achieve the objectives of the system, all sensors are fully autonomic to obtain product information from different locations in the traceability system and forward the information to the fog to maintain integrity and robustness in the system by utilizing historical data. The addition of this security element in the CPS is the motivation for secure food traceability [14]. The data for this research were CPS sensors, which work to obtain and forward product information securely to fog computing. Then, the system obtains the essential product information from the sensors where the collected information is fully protected from modification attacks. The novelty of the FogAuth-FT mechanism can be summarized as follows:

i. The integration of novel fog modules with the CPS-based food traceability system for the identification of poor-quality products from the supply chain by maintaining reliable product information to increase the trust level;
ii. The utilization of novel sensing features along with monitoring and interface layer to gather product information from different layers to maintain the product's actual information;
iii. To maintain the integrity, the details captured by the sensors along with the distribution of the information collected from the monitoring layers and stored in the fog;
iv. The utilization of a hybrid authentication mechanism with the integrated modification ability wherein the system can select users' authentication criteria.

The remainder of article is structured as follows: Section 2 defines the existing studies related to food traceability and the CPS environment. Section 3 explains the proposed traceability system, as well as the details of the proposed technique. Section 4 exhibits the experimental results. Finally, Section 5 concludes the paper and gives future insights.

2. Related Work

As the CPS supports every field of our daily life and also provides a variety of features, it has become a popular emerging technology. Due to this, the CPS faces various challenges according to its physical and logical nature [15]. According to these challenges, the research community is trying to address these issues and find the best possible solution. With the advancement of technology in terms of computing, communication, and the controlling

system, the CPS is a requirement of the current era [16]. The CPS is an emerging tool to provide services in different fields. However, its security is one of the significant research topics [17]. Furthermore, before starting research on the CPS, a deep knowledge of modern technology, network approaches, controlling systems technology, connectivity and communication technology, the physical environment, real-world objects, and other related fields is needed to improve the CPS technology, such as its real-time processing, self-sufficiency, system safety and security, and performance [18].

As the CPS supports various fields and provides a variety of features, it has become an emerging technology [19]. Due to this, the CPS faces various challenges according to its physical and logical nature. According to these challenges, researchers are trying to address these issues and find the best possible solution [20]. According to the design and framework of the CPS, various safety and security challenges are faced [21]. Its integration is based on those components that are prone to attack. The aim of the CPS is to provide a reliable environment for communications, as well as for data collection, which is the goal of every manufacturer in the market. Due to the Internet and other new technologies, everyone finds their desires on their smart phones. Thus, the CPS should maintain and forward reliable information inside the network.

As provided in [20], confidentiality, integrity, availability, and authenticity are the major challenges for a computing society to increase the security level and provide a free platform for the implementation of a CPS. Mostly, it is implemented in industries [22], automation [23], transportation [24], healthcare [25], and food traceability in the supply chain [26]. These all are more critical and crucial areas according to the confidentiality of data, the environment, and the resources. Therefore, data and account security methods are used for securing product information. In the literature, various techniques have been discussed for data security, e.g., eavesdropping, data tempering, and others [27]. Several studies have been published considering fog-computing-based food traceability, such as [28], and food information breach is a major issue in these systems. This section elaborates the existing approaches, whereas the contributions and limitations of these approaches are illustrated in Table 1.

Table 1. Contributions and limitations of the existing approaches.

Approach	Contribution	Limitation
[29]	Use of video surveillance cameras along with a novel dynamic background model for object monitoring.	Compression and decompression of stream data may take excessive time.
[30]	Creation of a 3D city model and utilization of deep learning for object identification.	Requires abundant resources.
[26]	Stream monitoring with fuzzy rules and stream mapping.	Integrity challenges due to the traceability database.
[31]	Utilization of fog computing to reduce latency and communication cost.	T-S fuzzy and ANN-based fog increases the computational complexity.
[32]	Division of layers into monitored, control, and cloud servers.	Depending on the cellular network and GPRS, may cause transmission delay.
[33]	IoT later to capture information with the fog and cloud.	Increased latency and transmission cost.
[34]	Utilization of real-time processing for prompt decision-making.	The A* algorithm is a blind search algorithm that may increase time and waste resources.

In [35], an intelligent approach was proposed for CPS-based predictive food traceability in agriculture fields. The approach utilizes an intuitionistic-based fuzzy case approach with an integrated enterprise architecture. The architecture of the proposed approach consists of a database, fuzzy membership function, traceable point, and fog computing. Another framework was proposed in [36] for traceability, which focused on small manufacturing companies. The proposed system has the capability to monitor the movements of companies in addition to controlling the system. The major contribution of the proposed approach is to generate real-time notifications whenever users make errors. In [37], a PetriNet-based mechanism was proposed to support traceability in a CPS. The architecture of this approach contains five layers, where the architecture integrates a dedicated data collection interface for inventory and dealers. The traceability interface is dedicated to consumers, by which they can trace the products.

In [29], a food traceability approach was proposed that works using video surveillance. The proposed approach utilizes a novel dynamic background model to define related subjects such as vehicles or people. Further, the trajectories for surveillance are generated by using different cameras. The significant contribution of the proposed mechanism is that the system generates image-based traceability information of the object, which enhances the analysis efficiency. However, video surveillance generates many data, and compression may increase the complexity and also requires a resource for decompression, making it a slow method. In [30], a food traceability approach was proposed that also extracts information by processing video surveillance data. The proposed system works in four steps; Firstly, it builds a 3D model of the areas that need to be monitored. Then, the system maps 2D views in the video cameras for the coordinate system. In the next step, a deep learning model is utilized for object identification to identify the targeted areas. Finally, cameras are utilized from multiple trajectories to generate unified traceability. The significant contribution of the proposed mechanism is the deep-learning-based identification along with the 3D city model to monitor products. However, formulating 3D models and generating 2D views with multiple cameras to generate traceability trajectories require abundant resources to perform the required processing.

In [26], an approach was proposed for stream-based food traceability using fog computing (Steam-FT). The proposed mechanism utilizes an enterprise architecture with EPCglobal and VSM for efficient traceability. In this mechanism, the fog-based CPS consists of several components, i.e., food production, logistics, and customer stakeholders with the handler, re-packer, and customer. The system implements the private, public, and CPS-based fog to work together for traceability. The transmission of data relies on a wireless sensor network (WSN) where the data are stored on servers. The proposed architecture utilizes fuzzy rules connected to the traceability database and distributes the CPS. It is further connected to an intelligent CPS using the EPCIS system. The main objective of the proposed mechanism is the utilization of the stream along with fuzzy rules and value stream mapping for efficient traceability. However, the food traceability database needs to be secure to maintain integrity, as it is accessible by distributors, retailers, and producers.

In [31], an intelligent inference was proposed using fog computing for integrated IoT in the food supply chain. The working of the proposed mechanism is divided into three components, i.e., performance evaluation system, T-S fuzzy inference, and ANN-based fog computing. The fog-based ANN uses a fuzzy inference system between the input/output simulated on a non-linear system for traceability. The important feature of the proposed mechanism is the utilization of an ANN-based fuzzy inference system at the fog layer. However, utilizing these in parallel increases the complexity of the system, which results in an inefficient utilization of the available resources. Another fog-computing-based intelligent approach was proposed in [38] to predict and prevent Zika virus. The proposed mechanism integrates fog computing, cloud computing, IoT-based sensors, and mobile phones to identify Zika virus. This approach utilizes fog computing to reduce the latency time, as well as extra transmission/communication cost. The fuzzy k-nearest neighbor algorithm was implemented to diagnose infected users.

Another traceability approach was proposed in [33], which integrates cloud and fog computing. The system also utilizes the IoT to collect and transfer information and store that information using the cloud. The major focus of the proposed study was to satisfy users' by addressing the challenges related to the condition, position, and quality of the product. The architecture of the proposed approach consists of the capture, fog, and cloud platforms. The capture platform contains capture nodes for capturing and transmitting information to the EPSIS capture interface at the fog layer. The fog layer then maintains a repository and processes the information in the query interface. The cloud layer includes data centers, the directory server, and the broker. The major contribution of the proposed mechanism is the utilization of the fog, cloud, and IoT together to capture information and utilizing the fog layer for storage and processing purposes. However, the utilization of

the fog and cloud may cause integrity issues and can increase the latency, in addition to notably increasing the communication cost.

In [32], a fog-computing-based approach was proposed to address the issues related to blackberry chain management. In this mechanism, the utilization of the fog was divided into two layers, where Layer 1 monitors and controls the supply chain and Layer 2 manages the cloud servers, where the communication is performed using the cellular or GPRS network. Another cloud–fog integrated architecture was proposed for an Internet-enabled supply chain [34]. The proposed approach utilizes A*, with real–time processing with enabled IoT and fog capabilities to manage the supply chain.

3. Proposed Traceability System

The proposed model captures the solutions for the emphasized problems faced by the supply chain and consumers. In this section, all elements of the proposed model and its deployment are elaborated. The model works on the supply chain to protect food products from any deception and modification attacks during the production processes. Furthermore, the proposed FogAuth-FT approach also provides reliable product information to the system and helps remove poor-quality products from the supply chain. Therefore, this increases the positive impression in the market and of consumers regarding the manufacturers and products. The supply chain consists of different phases, where each phase is a step towards the completion of the product.

Thus, it is a serious issue to monitor every phase of the supply chain and its network while sharing data among the sensors. Since the food supply chain is working under the CPS for monitoring all phases and products, due to its different phases, various people are involved in interacting with the system and its resources. Therefore, it is very essential to secure the system, resources, and applications from all unauthorized access. The importance and sensitivity of food are based on the time period, which is also called the shelf-life of products.

Whenever a food product is used before the expiry of its shelf-life, it is healthy and effective for consumers. However, when the same product is used after the completion of its shelf-life, it is more dangerous to human health [39]. Such types of food products cause some serious issues, which may lead to death. Therefore, the proposed model protects the food supply chain from such types of issues regarding health caused by forwarding the wrong information. Moreover, the model removes poor-quality products from the supply chain, which increases the trust in and reliability of the products among consumers.

3.1. Requirements, Identification, and Tracking

This section illustrate the proposed approach's requirements along with food place and product identification during manufacturing, followed by the working mechanism of product movement tracking, as illustrated below:

i. Requirements: The food product traceability solution is based on three basic requirements, i.e., place identification, food product identification, and tracking movement;
ii. Food place identification: During the production process in the food supply chain, it is important to trace every involved phase uniquely. As we know that food products start from raw materials and then move step-by-step to completion, this should be traceable by anyone. In the supply chain, a food product changes its location time-to-time till completion; therefore, the location needs to be identified;
iii. Food product identification: It is also important to track and trace a food product throughout the supply chain. From the raw materials, i.e., from the initial phase till finishing, it must be distinctively identified;
iv. Movement tacking: The movement of food is very important to track and trace. It is the actual key element in the supply chain to be monitored during its production [40].

3.2. CPS-Based Secure Food Traceability Architecture

A CPS-based food traceability for fog computing model is proposed for the security of the food supply chain. The system is responsible for monitoring and maintaining resource information integrity. The CPS-based traceability model collects product information from the physical world and processes it before sharing with the fog. Then, this encrypts and forwards it securely to the next phase for the production and consumers' facilitation. The same process is performed during all phases of the supply chain to protect the system and its resources from any illegal modification attacks. In case of any legal change, the manufacturer should login through an authorized username and password, which is based on some secret questions. The CPS-based secure food traceability system for fog computing consists of multiple layers, i.e., real-world layer (physical world), sensing layer, virtual storage layer, monitoring layer, and intermediate layer, as presented in Figure 1. The working of these layers is elaborated below:

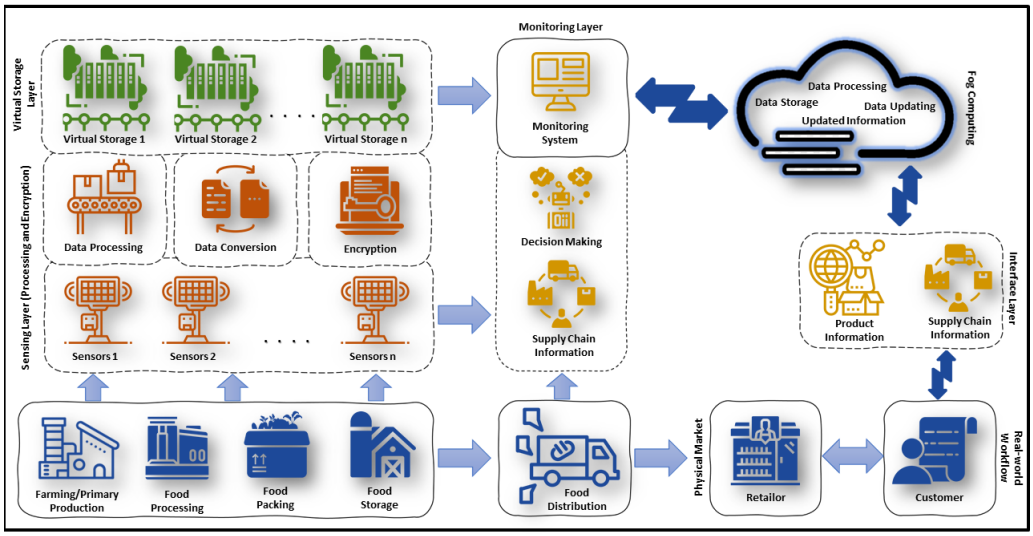

Figure 1. The proposed cps-based food traceability system.

i. Real-world layer: This is the ground or physical-world layer where the actual processes are performed physically. These processes consist of farming production where farmers produce the products, followed by the food processing layer, food packaging, and food storage. After this, the food is distributed to the retailer where customers can buy and are also able to obtain the product information from the intermediate layer;

ii. Sensing layer: The sensing layer is the primary layer equipped with the CPS sensors placed at different geographical locations of the supply chain. The CPS sensors consist of three main components, i.e., communication, computation, and control. The major functions performed at this layer are data processing, data conversion into operations, and encryption. The encryption and decryption are performed through the Twofish algorithm using a 256 bit key. In every phase of the supply chain, sensors are placed at different locations, which can sense the actual product information in an explicit form. This layer is further connected to the virtual storage layer;

iii. Virtual storage layer: The encrypted data transmitted by the sensing layer are sent to the virtual storage devices, and a copy of the information is forwarded to the parallel layer for monitoring purposes. Furthermore, the sensing layer is connected to virtual storage and communication devices to exchange content between the below and above layers. A virtual storage layer can also be utilized for collecting food product data. The key responsibility of the virtual layer provides services to the top layer for decision-making in addition to providing the facility to monitor the supply chain during the production process;

iv. Monitoring layer: The monitoring layer is the most significant one for food traceability because it is connected to the sensing layer and virtual storage layer and also gathers the information directly from food distribution vehicles. The monitoring layer has two significant components, i.e., decision-making and supply chain information. The incoming information from the sensing, virtual storage, and food distribution layers is integrated using supply chain components and forwarded to the decision-making components to evaluate the accuracy of the product information. The collection of information from different layers for evaluation purposes makes the proposed mechanism robust against modification attacks;

v. Interface layer: This layer provides an interface to consumers, which contains food supply chain information regarding the product quality, name, manufacturing date, expiry, and weight. If customers find all information on the Internet and the same product is delivered to them, then it increases the trust and reliability among them. If there is any ambiguity in the object information, then it will cause a negative impression for the consumers and markets, which may ultimately reduce the trust.

3.3. Twofish-Algorithm-Based Data Encryption

It is significant to secure the data sensed at the sensor layer to maintain the integrity of the information. The proposed approach utilizes the Twofish algorithm to encrypt the sensed information. This section discusses the encryption and authentication processes. The significant features of the Twofish algorithm are the encryption using a block size of 128 bit, which can accept a key length up to 256 bit, and the great efficiency, due to which it can be implemented on both hardware and software platforms. This algorithm has several noteworthy features, i.e., it accepts additional key lengths and also provides variety for more applications. The Twofish design supports both analysis and implementation [41]. This algorithm is designed for better performance, i.e., it efficiently works on a variety of platforms and fields as it only requires a 32 bit CPU, 8 bit smart card, and small/large-scale circuits. The design of Twofish permits various layers of performance. It depends on the encryption processing speed, key size, use of memory, hardware, and other parameters for implementation. The outcome of its performance is used in different applications of cryptography [41].

The FogAuth-FT mechanism utilizes the Twofish algorithm at the sensing layer and in fog computing to encrypt the data sensed from the physical ground layer. The fog encrypts the data received from the interface layer and later performs data mining, as discussed in Section 3.4. When the plaintext is received, the Twofish algorithm performs 16 rounds, where in each round, 32 bit words serve as the input to the algorithm encryption function. As the fog is connected to the interface layer by which the customers can share their feedback, it is significant to authenticate customers before they share their opinions regarding any specific product. Moreover, customer feedback is an important feature used by the decision-making layer; thus, it validates the customers before giving access to them. To authenticate customers, the proposed mechanism provides the capability of account verification by which users/customers can verify their accounts to update their feedback record related to any particular product using their unique identity. The verification process of users is implemented using a hybrid user authentication mechanism, i.e., the username (unique id), traditional alphanumeric password [42], graphical pattern image generation [43], and biometric authentication, which can be an iris scan, fingerprint, a retina scan, etc. [44]. Biometric authentication consists of three options (as mentioned earlier), and it is the choice of the system to select any of the processes for authentication. The complete authentication process of users/customers is illustrated in Algorithm 1.

Algorithm 1 Hybrid user authentication process.

procedure INITIAL LOGIN PROCESS($User_{id}$)
  $U_{id} \rightarrow$ input username ▷ User enters a pre-selected username
  $U_{pass} \rightarrow$ input password ▷ User enters a pre-selected alphanumeric password
  if (U_{id}&&U_{pass} == True) **then** ▷ Decision-making
    Go to the next procedure;
  else
    discard process; ▷ Discard the process
procedure GRAPHICAL AUTHENTICATION(D_{trust}^{n-id})
  $U_{fr1} \rightarrow$ Select first-round image ▷ Image selection from canvas
  $U_{fr2} \rightarrow$ Select second image
  $U_{fr3} \rightarrow$ Select second image
  if (U_{fr1}&&U_{fr2}&&U_{fr3}) == True **then** ▷ Decision-making
    Go to the next procedure;
  else
    discard process; ▷ Discard the process
procedure BIOMETRIC AUTHENTICATION(U_{bio}) ▷ Biometric authentication process
  $U_{ir} \rightarrow$ Iris scanning ▷ Iris-based authentication
  $U_{re} \rightarrow$ Retina scanning ▷ Retina-based authentication
  $U_{fp} \rightarrow$ Fingerprint scanning ▷ Finger-based authentication
  if ($U_{ir}||U_{re}||U_{fp}$) == True **then** ▷ Final decision-making
    Allow user to make changes;
  else
    discard authentication process; ▷ Unsuccessful authentication
Exit

3.4. Utilization of Fog Computing in the Proposed CPS

The FogAuth-FT food traceability system also utilizes fog computing to enhance efficiency and to improve the integrity for the quick identification of a modification attack along with other features. Most of the existing approaches have utilized fog computing to reduce the latency or communication cost by the proposed mechanism integrating several distinct components. The proposed mechanism integrates four modules, i.e., application, big data storage, big data mining, and decision-making modules as illustrated by Figure 2. The application module is further divided into two modules, i.e., vendor notification and farmer notification. This model was added to improve the working efficiency of both vendors and farmers by updating them with the areawise product detail and requirement followed by the notifications related to weather conditions and disease to the farmers. Furthermore, the next module of the fog is big data storage, where the gathered data are stored in encrypted form using the Twofish algorithm. Data in this module can be used by the decision-making module during the formulation of decisions related to any specific product. Data in this module consist of farmer-formulated data, distribution data related to the product and retailer, supply chain information, marketing agency data, product manufacturer data, and user/customer feedback. The next module (big data mining) performs a significant role in food traceability by using the product quality, requirement, and disease information to trace the poor-quality food.

All the previously discussed modules rely on the sensed data transmitted by the sensing layer and by the monitoring layer to the fog, where the decision-making module receives the required data from these modules to perform the required operations. The information used by this module is product information such as manufacturing information, delivery information, expiry date, product weight, and user feedback to make decisions. This layer performs the key operations, as its decision can increase or decrease the reputation/trust of the customers towards retailers or owners of the companies.

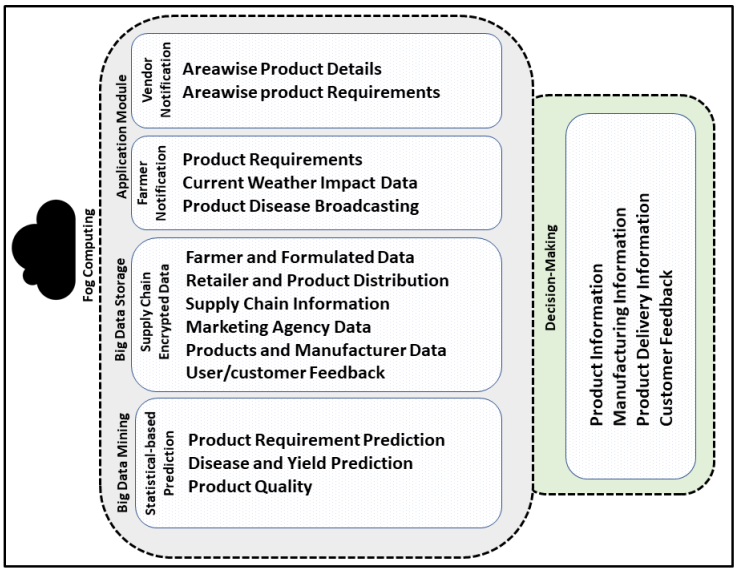

Figure 2. The integration of fog computing into the FogAuth-FT food traceability system.

4. Simulation Environment

This section elaborates the simulation outcome to achieve the three main objectives of the proposed model as mentioned earlier. The results were generated according to the three main key elements of the CPS-based secure food traceability system. These key factors are encryption time, computational cost, and attack protection. The result of the key factors was then compared with Stream-FT [26] and FogCloud-FT [33]. The tool used to simulate the proposed mechanism was iFogSim [45], which is an open-source toolkit for network simulations, such as the edge, fog, and cloud. The encryption time was evaluated under different scenarios, i.e., with 128 bit, 192 bit, and 256 bit key sizes, as discussed in Section 4.1.

4.1. Encryption Time

The encryption of product information is an important factor of the CPS-based secure food traceability system. The process of encryption and decryption in minimum time increases the production for supply chain. Encryption and decryption are useful and critical parameters of a secure food traceability system. The average analysis of the simulation outcome with 192 bit and 256 bit block sizes is presented in Table 2.

We implemented the Twofish algorithm in the proposed architecture and compared it with the existing approaches. In Figure 3, we take a key size of 128 bit and a block size of 192 bit for the three different techniques, i.e., proposed approach, Stream-FT, and FogCloud-FT. Therefore, we encrypted the same size and key plaintext with the three different techniques. FogAuth-FT performed the same task in less time as compared to others, where the encryption time was measured in milliseconds (ms). The proposed approach consumed 60 ms to encrypt the plaintext with a 128 bit key and a 192 bit block size.

In Figure 4, we take the key and block sizes as 192 bit for the three techniques, where Twofish performed the same task in less time compared to the others. In Figure 5, we take a key size of 256 bit and a block size of 192 bit to check the efficiency of the Twofish algorithm. For every encryption of the plaintext, it took 16 rounds. Twofish performed better for these key and block sizes. In Figure 6, we measured the encryption time by changing the key and block sizes. We took a key size of 128 bit and a block size of 256 bit to evaluate the performance. In Figure 7, we took a key size of 192 bit and a block size of 256 bit to evaluate the performance.

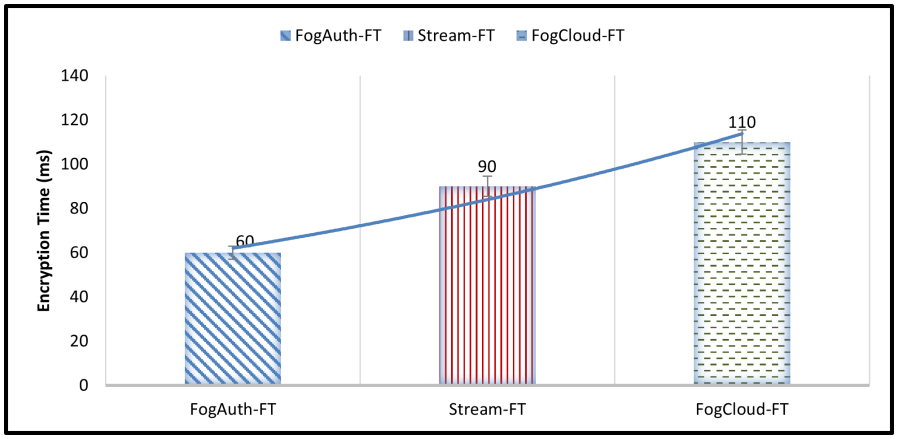

Figure 3. Encryption time with a key size of 128 bit and a block size of 192 bit.

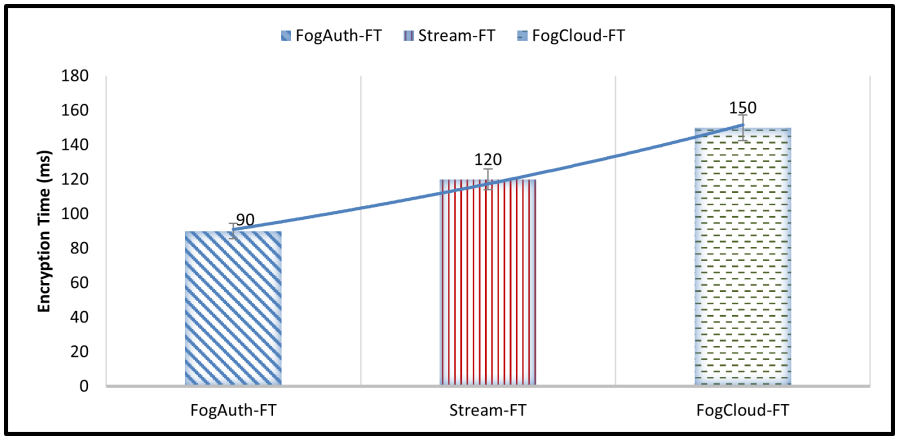

Figure 4. Encryption time with key size 192 bit and block size 192 bit.

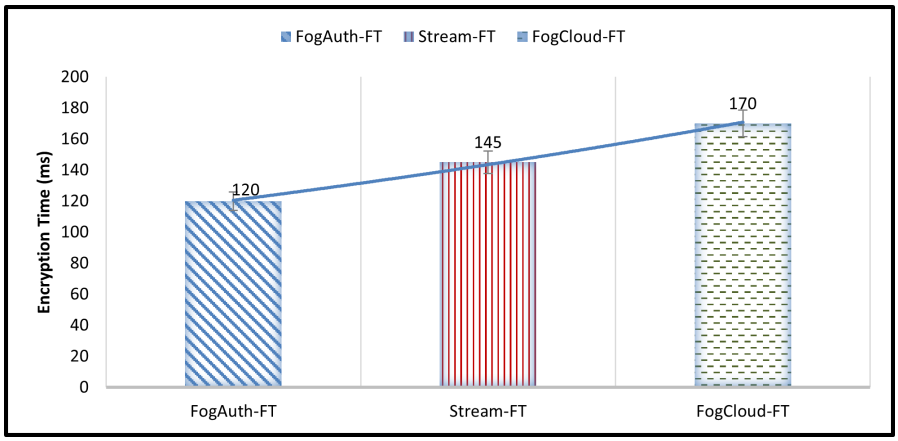

Figure 5. Encryption time with key size 256 bit and block size 192 bit.

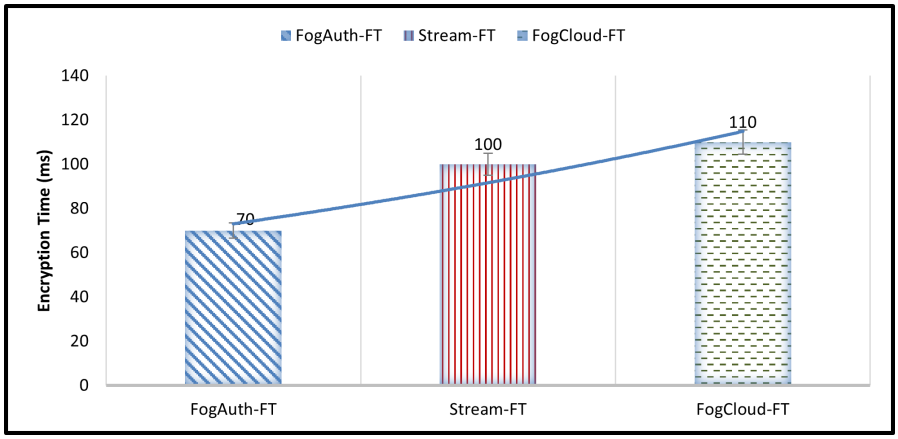

Figure 6. Encryption time with key size 128 bit and block size 256 bit.

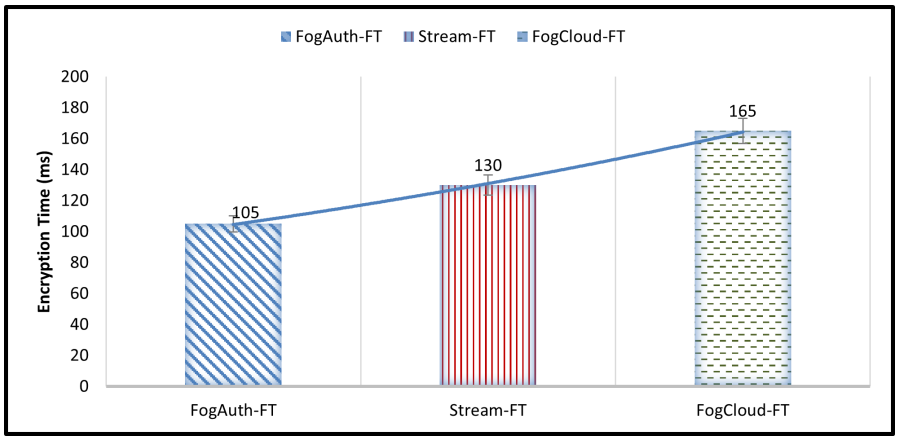

Figure 7. Encryption time with key size 192 bit and block size 256 bit.

In Figure 8, we took key and block sizes of 256 bit for the performance evaluation. It is obvious from Figures 3–8 that the FogAuth-FT algorithm performed better with different key and block sizes.

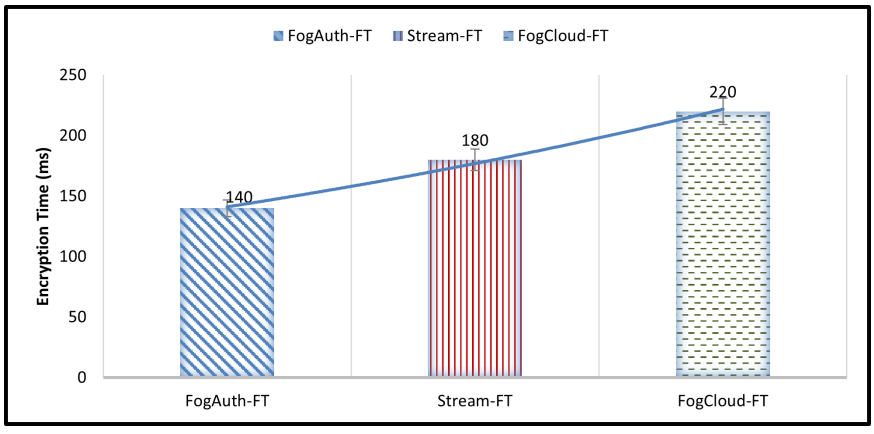

Figure 8. Encryption time block sizes of 256 bit.

Table 2. Average analysis of FogAuth-FT with a block size of 192 bit and 256 bit.

Block Size	192 bit			Average Percentage
Key Size	128 bit	192 bit	256 bit	
FogAuth-FT	60	90	110	86.67
Stream-FT	90	120	150	120
FogCloud-FT	110	145	120	125
Block Size	256 bit			Average Percentage
Key Size	128 bit	192 bit	256 bit	
FogAuth-FT	70	105	140	105
Stream-FT	100	130	180	136.67
FogCloud-FT	110	165	220	165

4.2. Trusted Data Identification and Error Estimation

Encryption helps to maintain the integrity as data arrive from different resources. It is significant to evaluate the performance to estimate the error percentage to validate that the data received from different resources are error free and can be utilized for future decision-making. The error estimation was performed on the sensed data transmitted by the sensors. In FogAuth-FT, the data collected by sensors at the sensed layer are transmitted to the virtual storage, whereas the monitoring layer holds and transmits the encrypted data to the fog. The error percentage estimation was performed on data transmitted to the fog by the monitoring layer. For this, the number of sensors placed were 10–145, which increased with time. The malicious percentage of the sensors was 30%, while the performance analysis was performed considering 128 bit, 192 bit, and 256 bit. Figure 9 illustrates the simulation outcome of the proposed mechanism. The result showed that with the increasing number of sensors, the error estimation percentage decreased and the integrity improved.

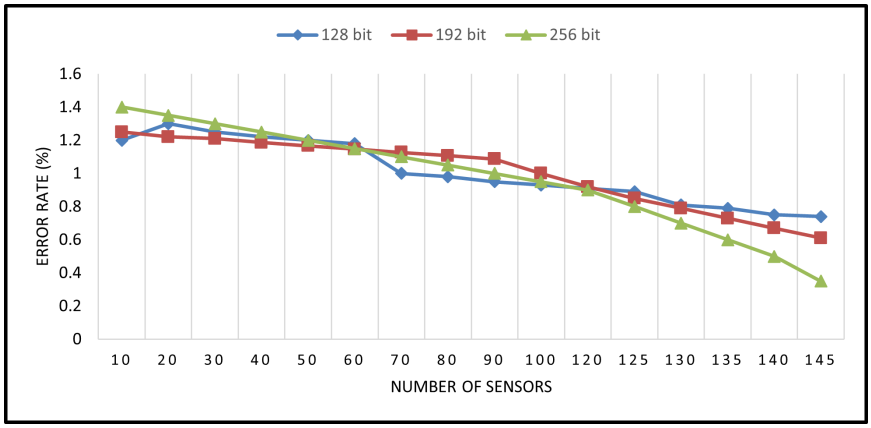

Figure 9. Error estimation percentage on the data received by the fog.

The identification of the feedback received by the users from the interface layer is also significant. If the received information is not trustworthy or the error rate increases, then it may affect the decision-making of the fog. The feedback is most critical as a few users can enter false information either purposefully or with the influence of their surroundings. In the proposed mechanism, the user feedback was compared to the data received by the monitoring layer to verify the information. For the identification of correct user feedback, the performance of the proposed mechanism was simulated with 5–145 users (which increased with time) and the encryption bits were 128 bit, 192 bit, and 256 bit. Figure 10 demonstrates the simulation outcome of the encrypted data. The result showed that the

identification rate was higher at the beginning; however, with the passage of time, the 256 bit encrypted data performed relatively better at detecting false information.

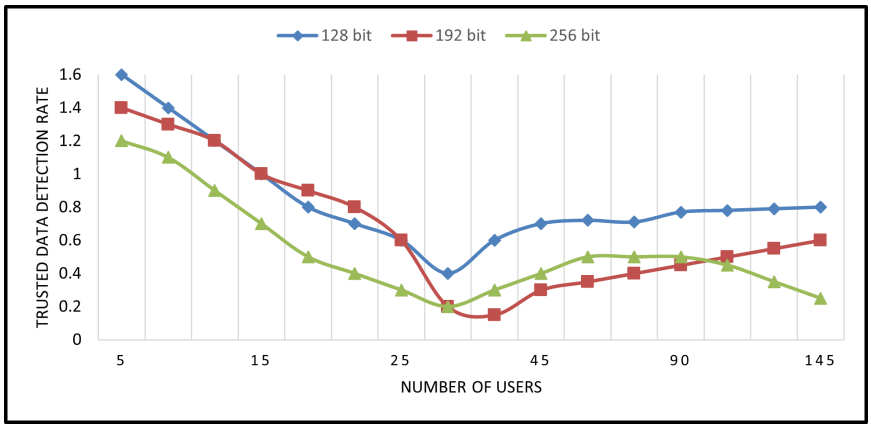

Figure 10. Detection of trusted data shared by the user using the interface layer.

4.3. Computational Cost

The computational cost is the key point of this research. This was evaluated on the basis of how much resource was required and used by the food traceability system while performing encryption and decryption. We used the Twofish algorithm for cryptography. We took different key and block sizes to measure the result and achieve the goal of this research. The basic aim of Twofish is to process various lengths of blocks and key sizes in a short span of time while using less resource.

Figure 11 represents the computational cost of encryption, which executes different sizes of blocks of data on different processors. Twofish implements and executes less memory on hardware such as CPUs and RAM and encrypts data in a short amount of time. The graph shows the results of the computational cost of Twofish, which was better than the others. The computational cost of FogAuth-FT was less in comparison to existing approaches. With 128 bit, the computational cost of the proposed mechanism remained 3000 ms, whereas the cost of FogCloud-FT reached 5000 ms. Moreover, with 256 bit encryption, the proposed approach consumed 5000 ms in comparison to 6400 ms and 8000 ms for Stream-FT and FogCloud-FT, respectively.

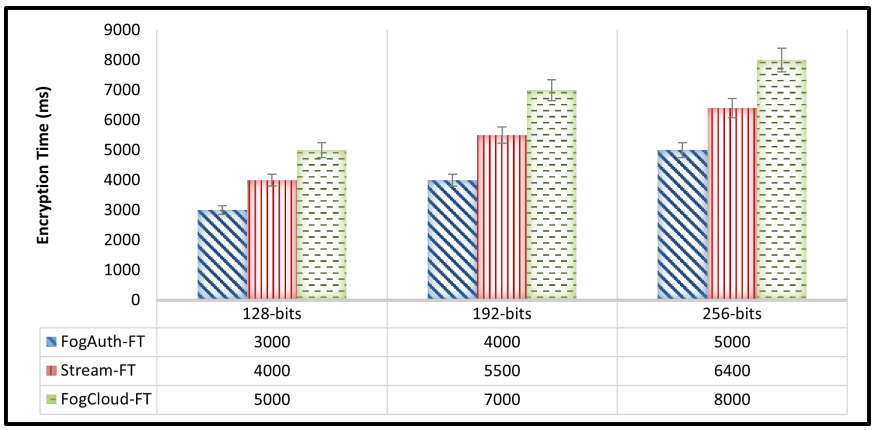

Figure 11. Comparison of computational resources utilized.

4.4. Modification Attack

The robustness evaluation against the modification attack is the last parameter to validate the model efficiency. This is the most important and key factor of the system according to sensitivity and system resources. We applied modification attacks at different layers to validate the performance. The simulation environment consisted of 450 min, whereas the

number of unauthentic nodes executing the modification attacks was 60 for the fist 250 min, which was increased to 150–450 min. Figure 12 illustrates the simulation outcome of the proposed mechanism. The result showed that the detection rate of the proposed mechanism was higher, whereas FogCloud-FT also performed better in comparison to Stream-FT.

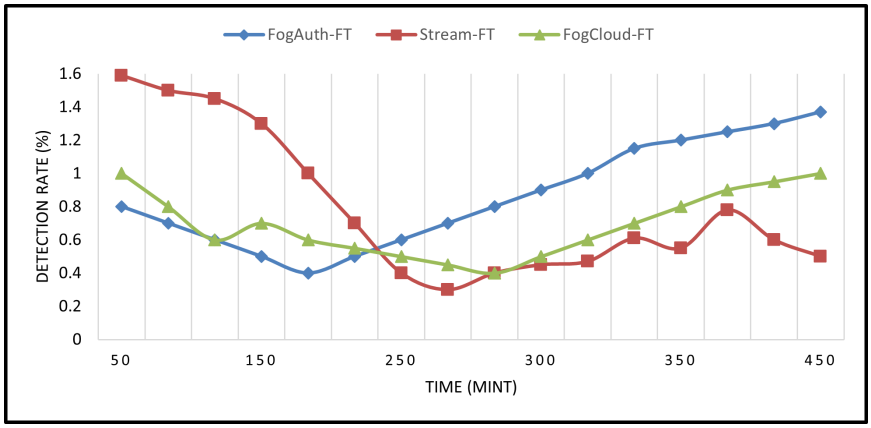

Figure 12. Robustness evaluation against the modification attack.

5. Conclusions

A CPS-based secure food traceability system has the potential to address the current challenges in the existing systems. Secure food traceability has the capability to protect the system from illegal modification and from unauthorized access. A food traceability approach was proposed that utilizes a cyber–physical system (CPS) and fog-integrated mechanism to address the existing challenges and to improve the overall workflow in the real-world by utilizing fog capabilities. The proposed approach integrates a novel fog module to perform several significant operations that not only address accurate traceability, but also facilitate farmers with enhanced production efficiency. Furthermore, to implement adequate robustness against illegal modification, the mechanism utilizes a hybrid approach to authenticate users before any modification. The proposed model has the capability to remove poor-quality products from the supply chain by detecting them through the monitoring layer and sensed information at the sensing layer. In addition, the model implements an interface layer to increase the consumers' trust level by providing accurate information and taking their feedback regarding the product. The simulation outcomes validated the performance of the proposed model where the Twofish algorithm along with fog-integrated modules performed better in terms of computational cost, modification attacks, and encryption speed, as compared to the eavesdropping and data-tempering techniques. In the future, the proposed technique can be applied to food traceability in name-based networking.

Author Contributions: Conceptualization, K.A.A., I.U.D. and A.A.; methodology, I.U.D. and A.A.; software, K.A.A.; validation, A.A.; formal analysis, I.U.D. and B.-S.K.; investigation, A.A. and B.-S.K.; resources, B.-S.K.; data curation, K.A.A.; writing—original draft preparation, K.A.A.; writing—review and editing, I.U.D. and A.A.; visualization, B.-S.K. and A.A.; supervision, I.U.D.; project administration, A.A.; funding acquisition, B.-S.K. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the National Research Foundation (NRF), Korea, under Project BK21 FOUR (F21YY8102068); and in part by King Saud University, Riyadh, Saudi Arabia, through Researchers Supporting Project Number RSP-2021/184.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Khattak, H.A.; Tehreem, K.; Almogren, A.; Ameer, Z.; Din, I.U.; Adnan, M. Dynamic pricing in industrial internet of things: Blockchain application for energy management in smart cities. *J. Inf. Secur. Appl.* **2020**, *55*, 102615. [CrossRef]
2. Smetana, S.; Aganovic, K.; Heinz, V. Food Supply Chains as Cyber-Physical Systems: A Path for More Sustainable Personalized Nutrition. *Food Eng. Rev.* **2021**, *13*, 92–103. [CrossRef]
3. Kim, T.; Yoo, S.E.; Kim, Y. Edge/Fog Computing Technologies for IoT Infrastructure. *Sensors* **2021**, *21*, 3001. [CrossRef]
4. Binti Azram, N.A.; binti Atan, R. SPL-based traceability model for food document tracing. In Proceedings of the IEEE 2015 9th Malaysian Software Engineering Conference (MySEC), Kuala Lumpur, Malaysia, 16–17 December 2015; pp. 212–216.
5. Asuncion, H.U.; François, F.; Taylor, R.N. An end-to-end industrial software traceability tool. In Proceedings of the 6th Joint Meeting of the European Software Engineering Conference and the ACM SIGSOFT Symposium on The Foundations of Software Engineering, Dubrovnik, Croatia, 17 September 2007; pp. 115–124.
6. Young, G. *Synthetic Structure of Industrial Plastics, in Plastics*; Peters, J., Ed.; McGraw-Hill: New York, NY, USA, 1964; Volume 3.
7. Shahid, A.; Almogren, A.; Javaid, N.; Al-Zahrani, F.A.; Zuair, M.; Alam, M. Blockchain-based agri-food supply chain: A complete solution. *IEEE Access* **2020**, *8*, 69230–69243. [CrossRef]
8. Antonides, G.; Hovestadt, L. Product attributes, evaluability, and consumer satisfaction. *Sustainability* **2021**, *13*, 12393. [CrossRef]
9. Hidayat, A.; Wijaya, T.; Ishak, A.; Endi Catyanadika, P. Consumer Trust as the Antecedent of Online Consumer Purchase Decision. *Information* **2021**, *12*, 145. [CrossRef]
10. Janjua, K.; Shah, M.A.; Almogren, A.; Khattak, H.A.; Maple, C.; Din, I.U. Proactive forensics in IoT: Privacy-aware log-preservation architecture in fog-enabled-cloud using holochain and containerization technologies. *Electronics* **2020**, *9*, 1172. [CrossRef]
11. Vidmar, D.; Marolt, M.; Pucihar, A. Information Technology for Business Sustainability: A Literature Review with Automated Content Analysis. *Sustainability* **2021**, *13*, 1192. [CrossRef]
12. He, S.; Chen, J.; Shu, Y.; Cui, X.; Shi, K.; Wei, C.; Shia, Z. Efficient Fault-tolerant Information Barrier Coverage in Internet of Things. *IEEE Trans. Wirel. Commun.* **2021**, *20*, 7963–7976. [CrossRef]
13. León-Bravo, V.; Caniato, F.; Caridi, M. Sustainability assessment in the food supply chain: Study of a certified product in Italy. *Prod. Plan. Control* **2021**, *32*, 567–584. [CrossRef]
14. Badia-Melis, R.; Mishra, P.; Ruiz-García, L. Food traceability: New trends and recent advances. A review. *Food Control* **2015**, *57*, 393–401. [CrossRef]
15. Poltavtseva, M.; Shelupanov, A.; Bragin, D.; Zegzhda, D.; Alexandrova, E. Key Concepts of Systemological Approach to CPS Adaptive Information Security Monitoring. *Symmetry* **2021**, *13*, 2425. [CrossRef]
16. Morella, P.; Lambán, M.P.; Royo, J.A.; Sánchez, J.C. The Importance of Implementing Cyber Physical Systems to Acquire Real-Time Data and Indicators. *J* **2021**, *4*, 147–153. [CrossRef]
17. Hammoudeh, M.; Watters, P.; Epiphaniou, G.; Kayes, A.; Pinto, P. Special Issue "Security Threats and Countermeasures in Cyber-Physical Systems". *J. Sens. Actuator Netw.* **2021**, *10*, 54. [CrossRef]
18. Thompson, D.R.; Rainwater, C.E.; Di, J.; Ricke, S.C. Student cross-training opportunities for combining food, transportation, and critical infrastructure cybersecurity into an academic food systems education program. In *Food and Feed Safety Systems and Analysis*; Elsevier: Amsterdam, The Netherlands, 2018; pp. 375–391.
19. Rani, S.; Kataria, A.; Chauhan, M. Fog computing in industry 4.0: Applications and challenges—A research roadmap. In *Energy Conservation Solutions for Fog-Edge Computing Paradigms*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 173–190.
20. Keerthi, C.K.; Jabbar, M.; Seetharamulu, B. Cyber Physical Systems (CPS): Security Issues, Challenges and Solutions. In Proceedings of the 2017 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Coimbatore, India, 14–16 December 2017; pp. 1–4.
21. Ali, W.; Din, I.U.; Almogren, A.; Guizani, M.; Zuair, M. A lightweight privacy-aware iot-based metering scheme for smart industrial ecosystems. *IEEE Trans. Ind. Inform.* **2020**, *17*, 6134–6143. [CrossRef]
22. Tao, H.; Bhuiyan, M.Z.A.; Rahman, M.A.; Wang, T.; Wu, J.; Salih, S.Q.; Li, Y.; Hayajneh, T. TrustData: Trustworthy and secured data collection for event detection in industrial cyber-physical system. *IEEE Trans. Ind. Inform.* **2019**, *16*, 3311–3321. [CrossRef]
23. Lv, C.; Hu, X.; Sangiovanni-Vincentelli, A.; Li, Y.; Martinez, C.M.; Cao, D. Driving-style-based codesign optimization of an automated electric vehicle: A cyber-physical system approach. *IEEE Trans. Ind. Electron.* **2018**, *66*, 2965–2975. [CrossRef]
24. Deka, L.; Khan, S.M.; Chowdhury, M.; Ayres, N. Transportation cyber-physical system and its importance for future mobility. In *Transportation Cyber-Physical Systems*; Elsevier: Amsterdam, The Netherlands, 2018; pp. 1–20.
25. Xu, J.; Wei, L.; Wu, W.; Wang, A.; Zhang, Y.; Zhou, F. Privacy-preserving data integrity verification by using lightweight streaming authenticated data structures for healthcare cyber–physical system. *Future Gener. Comput. Syst.* **2020**, *108*, 1287–1296. [CrossRef]
26. Chen, R.Y. An intelligent value stream-based approach to collaboration of food traceability cyber–physical system by fog computing. *Food Control* **2017**, *71*, 124–136. [CrossRef]
27. Feng, H.; Wang, X.; Duan, Y.; Zhang, J.; Zhang, X. Applying blockchain technology to improve agri-food traceability: A review of development methods, benefits and challenges. *J. Clean. Prod.* **2020**, *260*, 121031. [CrossRef]
28. Adnan, M.; Lu, Y.; Jones, A.; Cheng, F.T. Application of the Fog Computing Paradigm to Additive Manufacturing Process Monitoring and Control. SSRN 3785854. 2021. Available online: https://ssrn.com/abstract=3785854 (accessed on 17 December 2021).

29. Mao, B.; He, J.; Cao, J.; Bigger, S.W.; Vasiljevic, T. A framework for food traceability information extraction based on a video surveillance system. *Procedia Comput. Sci.* **2015**, *55*, 1285–1292. [CrossRef]
30. Mao, B.; He, J.; Cao, J.; Gao, W.; Pan, D. Food traceability system based on 3d city models and deep learning. *Ann. Data Sci.* **2016**, *3*, 89–100. [CrossRef]
31. Chen, R.Y. Fog computing-based intelligent inference performance evaluation system integrated internet of thing in food cold chain. In Proceedings of the IEEE 2015 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), Zhangjiajie, China, 15–17 August 2015; pp. 879–886.
32. Musa, Z.; Vidyasankar, K. A fog computing framework for blackberry supply chain management. *Procedia Comput. Sci.* **2017**, *113*, 178–185. [CrossRef]
33. Mededjel, M.; Belalem, G.; Neki, A. Towards a traceability system based on cloud and fog computing. *Multiagent Grid Syst.* **2017**, *13*, 47–68. [CrossRef]
34. Mededjel, M.; Belalem, G.; Neki, A. A cloud-fog architecture for physical-internet-enabled supply chain. *Supply Chain. Forum Int. J.* **2021**, *32*, 1–16. [CrossRef]
35. Chen, R.Y. Intelligent predictive food traceability cyber–physical system in agriculture food supply chain. In *Journal of Physics: Conference Series*; IOP Publishing: Avid College, Maldives, 2018; Volume 1026, p. 012017.
36. Bordel Sánchez, B.; Alcarria, R.; Martín, D.; Robles, T. TF4SM: A framework for developing traceability solutions in small manufacturing companies. *Sensors* **2015**, *15*, 29478–29510. [CrossRef] [PubMed]
37. Huang, J.; Zhu, Y.; Cheng, B.; Lin, C.; Chen, J. A PetriNet-based approach for supporting traceability in cyber-physical manufacturing systems. *Sensors* **2016**, *16*, 382. [CrossRef]
38. Sareen, S.; Gupta, S.K.; Sood, S.K. An intelligent and secure system for predicting and preventing Zika virus outbreak using Fog computing. *Enterp. Inf. Syst.* **2017**, *11*, 1436–1456. [CrossRef]
39. Lin, Q.; Wang, H.; Pei, X.; Wang, J. Food safety traceability system based on blockchain and EPCIS. *IEEE Access* **2019**, *7*, 20698–20707. [CrossRef]
40. Bhatt, T.; Buckley, G.; McEntire, J.C.; Lothian, P.; Sterling, B.; Hickey, C. Making traceability work across the entire food supply chain. *J. Food Sci.* **2013**, *78*, B21–B27. [CrossRef]
41. Schneier, B.; Kelsey, J.; Whiting, D.; Wagner, D.; Hall, C.; Ferguson, N. Twofish: A 128-bit block cipher. *AES Submiss.* **1998**, *15*, 23–91.
42. Herrera-Macías, J.A.; Legón-Pérez, C.M.; Suárez-Plasencia, L.; Piñeiro-Díaz, L.R.; Rojas, O.; Sosa-Gómez, G. Test for Detection of Weak Graphic Passwords in Passpoint Based on the Mean Distance between Points. *Symmetry* **2021**, *13*, 777. [CrossRef]
43. Khan, M.A.; Din, I.U.; Jadoon, S.U.; Khan, M.K.; Guizani, M.; Awan, K.A. G-RAT | a novel graphical randomized authentication technique for consumer smart devices. *IEEE Trans. Consum. Electron.* **2019**, *65*, 215–223. [CrossRef]
44. Awan, K.A.; Ud Din, I.; Almogren, A.; Kumar, N.; Almogren, A. A Taxonomy of Multimedia-based Graphical User Authentication for Green Internet of Things. *ACM Trans. Internet Technol. (TOIT)* **2021**, *22*, 1–28. [CrossRef]
45. Gupta, H.; Vahid Dastjerdi, A.; Ghosh, S.K.; Buyya, R. iFogSim: A toolkit for modeling and simulation of resource management techniques in the Internet of Things, Edge and Fog computing environments. *Softw. Pract. Exp.* **2017**, *47*, 1275–1296. [CrossRef]