

Research Article

Study on Traceability System of Athletes Food Safety Based on Trusted Computing

¹Hongjiang Wu and ²Haiyan Zhao

¹Department of Sports, Northwest University, Xi'an 710069, China

²Department of Network Service, Xi'an Communication Institute, Xi'an 710106, China

Abstract: How to effectively prevent food contamination and foodborne diseases and the incidence of foodborne doping is one of the issues of the majority of coaches and athletes, which are of most concern. In the traditional food safety traceability system, how to ensure the information transfer process will be a difficult problem to solve. In this study, the trusted computing theory is applied to computer software system and it also proposes the thinking of three flow integration on athlete's food safety traceability system. Taking meat for an example, this study also proposes the thinking of multi-layer software architecture system as a whole and messaging security, etc.

Keywords: Athlete, food safety, traceability system, trusted computing

INTRODUCTION

In recent years, food contamination problems have seriously affected the athletes' health and reasonable dietary nutrition. Food poisoning or a positive doping test event happens from time to time due to eating contaminated food, overshadowing the athletes' training and competition and posing a great threat to fair competition sports (Luan *et al.*, 2012). Therefore, the establishment of reasonable and effective food safety traceability system is important to ensure the safety of athletes diet.

The main problem of traditional food traceability system is that it's stuck in the traceability of information. However, in food safety traceability system, traceability information is only one aspect, it's more important to ensure the credibility of information transmission. That is to say, the information will not be tampered within the transmission and distribution process, which is the most critical issues of athletes' food safety traceability. Three proposed architecture flow integration is an important way to ensure reliable transmission of information. And the establishment of improved functional, structural reusability of third-integrated system models with higher food safety traceability and the assessment of its functional elements and non-functional elements solve the flow of information and the credibility of the amount of the transfer process and also provide technical support and theoretical support in a wider range for system applications.

MATERIALS AND METHODS

Definition of trusted computing: Experts from various fields define the "credible" in terms of providing

services, key elements and behavioral targeting, in general, these definitions include the following in common (Shen and Zhang, 2007):

- Services provided by the computer system is reliable and this is arguably reliable.
- The goal is to meet the customer's trust, security, privacy, reliability and business reputation of the four key elements involved.
- Whether an entity can be trusted depends on whether it can achieve the stated objectives (action or behavior) along the expected way.

Relations between trusted computing and security:

Trusted computing and security are complementary, interdependent. Trusted computing makes up for the deficiencies of the security mechanisms' unstable foundation while the security mechanisms provide supplementary support for trusted computing, enabling a trusted computing environment in a complex practical and providing services to the upper layer. Therefore, in designing the important security architecture of information systems, the trusted computing and security must be closely combined, working together for system security services.

Related theoretical model:

Trust chain transfer model: Trust chain transfer is a credible departure from the body, determining the exact properties of the body around the object by means of a reliable method (algorithm) to ensure that the system functions composed of the subject and object is safe (Chen, 2006). In the trusted computing platform, the building and delivery of the trust chain involves three basic concepts. The first one is the trusted root; the

second is credible to pass; the third is credible measurement (Liang, 2008).

No interference model: The ideas of the no interference information flow were first proposed in 1982 by Goguen and Meseguer (1982). The idea can be understood as: if the main subject S1 has no effect on what the main subject S2 sees and does, it will be defines as no interference (Ma *et al.*, 1997).

Interference discovery mechanism: The so-called interference discovery mechanism is when interference occurs within the measurement range, interference mechanism can find it in time, give the appropriate treatment, to ensure the establishment of food safety traceability information environment circulation system.

RESULTS AND DISCUSSION

Definition of three streams: The so-called third-rate, refers to logistics, information flow and control flow.

Logistics: Refers to the process of circulation of food from production to the table during the athlete-related products.

Information flow: Refers to food-related attribute information in the planting, harvesting, processing and transportation of various stages. Includes two types of information, one is traceability information for traceability of food sources; the other is the basic information for the specific situation record producers, operators, consumers and the product itself.

Flow control: control flow is in the process of food circulation to achieve control of information and to ensure the operation legality, legitimacy and safety in the every step of food distribution process by taking appropriate means of control.

Relations between the three streams: Among the traditional food traceability systems, logistics and information flow is generally independent of each other. Both the security of information in a reliable logistics links and whether it will be tampered with can not guaranteed. In the architecture model to be established, logistics and information flow of information in all aspects of the implementation can be monitored and managed by increasing the control flow. It maintained the independence of logistics and information flow of the original form, but also enhance the three streams intrinsic link between each other, forcing them into a whole.

Three flow integration process applications: Starting from the cattle breeding stage, the case described the integration of third-meaning and characteristics. Logistics process includes purchase feed and medication, calves into the house, young cattle rearing and fattening, exporting and carrying cattle. The main carrier to trace the information in this phase is the signs on the cattle ears. Control flow information management includes procurement, feeding information management, traceability information management, synchronization monitoring and management, quarantine ledger management. Three flow integration process in this phase is shown in Fig. 1.

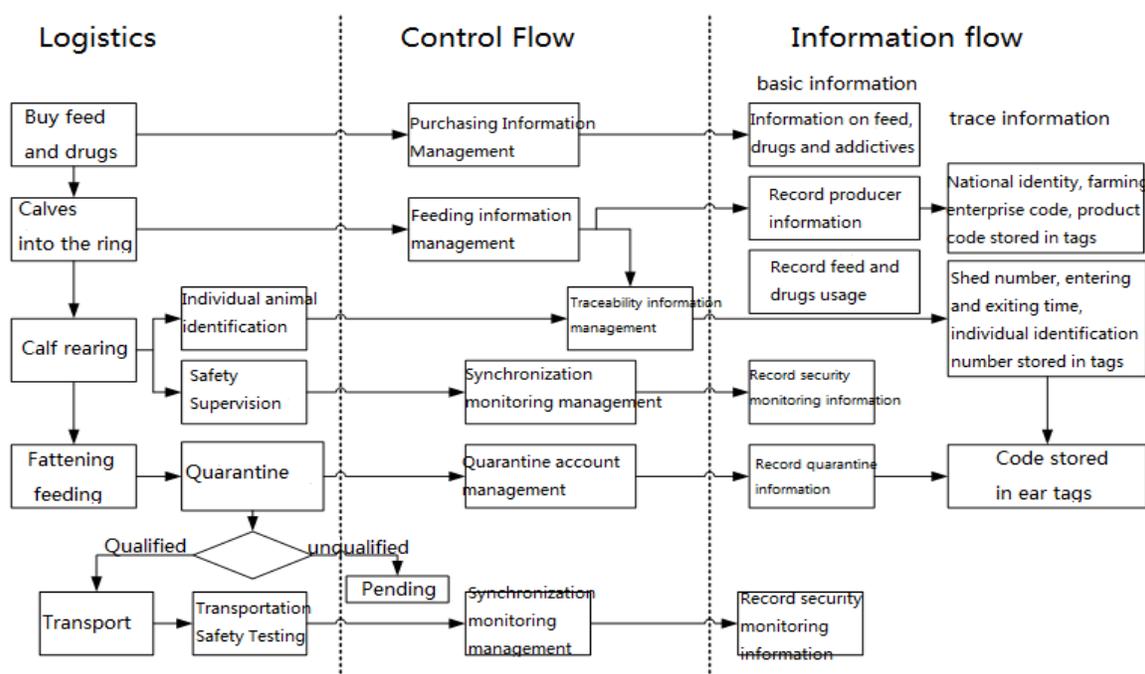


Fig. 1: Flow chart of three streams in integrated farming stage

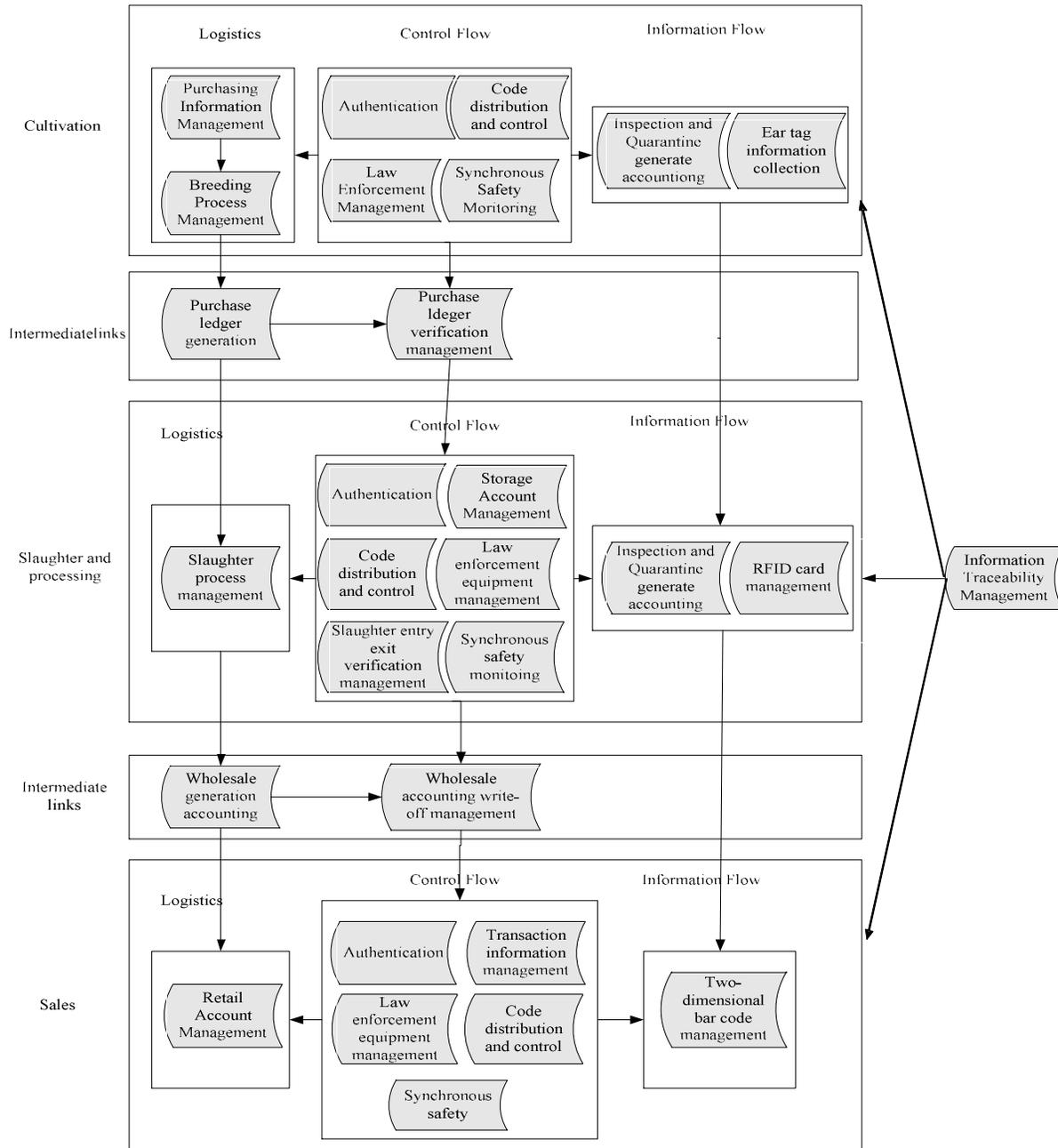


Fig. 2: Component classification chart

Credible idea in the design of components and reflect: Starting from food safety traceability system business requirements, abstract the components needed in the breeding, slaughter and processing, sales stage. These components also follows the integration of third-thinking logistics and can be divided into components, information flow and control flow component members, shown in Fig. 2.

Purchase ledger control member includes verification flow management, verification management ledger wholesale slaughter verification, retail verification, authentication and so on. Code

distribution and control provides the system with a trusted root-back yards, through verification algorithms to ensure consistency and control information at each stage of delivery. Once the system has a loss of data or inconsistent, the system will immediately remind to avoid causing damage to the eaters. That is the principle mechanism of interference found in this case, an important manifestation.

Based on component technology three flow integration software architecture: The system is designed with multi-layer software architecture

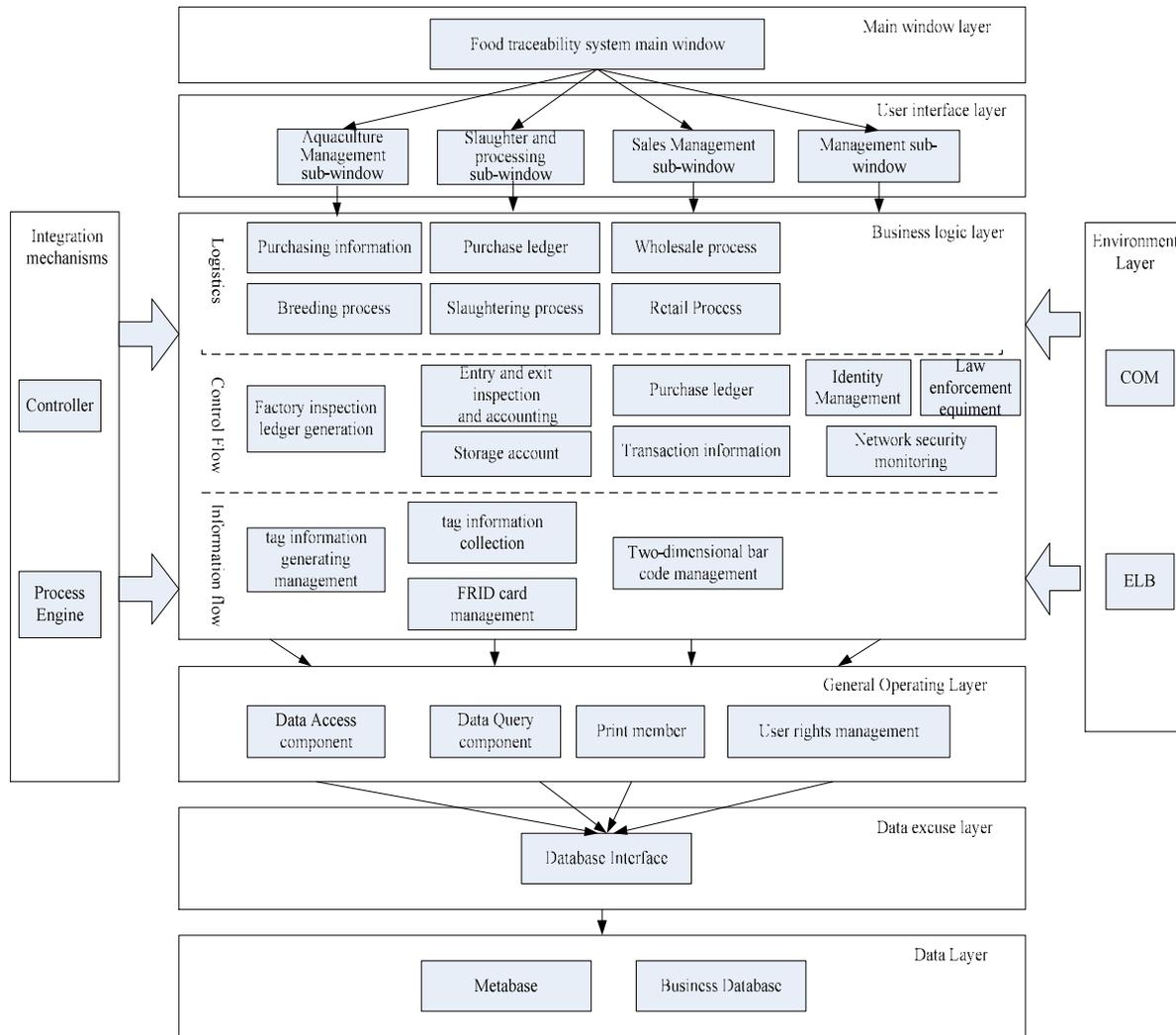


Fig. 3: Meat food safety traceability system multi-layer software architecture diagram

framework as a whole, including the user interface layer, business logic, common operating level, the data interface layer and data layer. Where in the user interface layer is composed of the interface object (UI object). It is the human-computer interaction interface, corresponding to the needs of users and is responsible for service triggering event to start the business logic; Business logic layer is the main application software systems, responsible for handling all the business logic and business rules directly related to operations; general operating layer logic layer is to provide some common features; data interface layer need to know the type of database server and its semantics interface, shielding the differences between the specific database server, thereby improving application portability and adaptability; data layer is the underlying software system, responsible for the storage and management of basic data and business data and these data are complete, consistency guarantee. Multi-layer software architecture diagram meat food safety traceability system is shown in Fig. 3.

Business logic safety information transfer:

Write-off between the subsystems: Because this system contains multiple subsystems, so whether the information transfer between systems conform credible chain transfer model requirements is an important indicator of the structural safety and reliability of system. Verification function between breeding and slaughter subsystem is achieved by ear tags and RFID card information management. The information checking between components ensures the information integrity and consistency in the circulation between the two states.

Encryption and decryption code: By tracing code structure reference existing similar products, GTIN (GTIN) +lot/serial number + source code entity reference will be adopted in beef food traceability code. In the process of designing back yards, a careful and reasonable encryption and decryption technology and technology necessary to recover broken code can eliminate the circulation of commodities malicious

destruction and tampering, which is an important manifestation of non-interference theory in control flow.

Safety data interface layer and data layer:

Authentication: All operating personnel accessing the system data must boot password, operating system password, the application password, database access password detection. The system will be strictly limited to the user's actions according to the client's IP address, operating employee number/password, books/warehouse number, etc.

Access control: The operation of the data in the database generally has input, query, edit, delete four cases. The users will be divided into four privilege levels and each operator can only operate the data within its purview.

CONCLUSION

Based on this new trusted computing idea, the proposal of athletes food safety traceability system multi-layer software architecture is bound to provide practical new ideas for developing and improving the food safety traceability system. Of course, it takes a

very long way to complete this architecture implemented into real athletes food safety traceability system, which needs training and supporting.

REFERENCES

- Chen, Y., 2006. Study on trusted computing model and architecture. Ph.D. Thesis, Wuhan University, Wuhan, China.
- Goguen, J. and J. Meseguer, 1982. Security policies and security models. Proceeding of the IEEE Symposium on Security and Privacy. IEEE Computer Society Press, Oakland, California, pp: 11-20.
- Liang, T., 2008. Based on the trusted computing platform of trust chain is reviewed. *Comput. Sci.*, 35(10): 15-18.
- Luan, Y.Q., Y.N. Zhang and X.Z. Wang, 2012. Clenbuterol and athlete food safety. *China Sports Coaches*, 2: 38-39.
- Ma, J.P., X.X. Yu and F. Hong, 1997. A complete no interference model. 20(11): 1034-1037.
- Shen, C.X. and H.G. Zhang, 2007. Overview of cyber security. *Sci. China*, 37: 129-150.