

Data security concepts for the NWCTI system



J. P. Thomas, C. C. Craige, M. D. Buser, and B. D. Adam

NWCTI-15

Oklahoma State University (OSU) has developed a traceability software system that interfaces with front-line traceability software packages. One of the primary stakeholder concerns related to such a system is data security. Security begins with defining a database structure and developing a management plan. Two fundamental database structures were considered for the National Whole Chain Food Traceability Institute (NWCTI) system: a distributed and a centralized database structure. In a distributed system, the data storage centers are spread across multiple locations. For example, the server at location 'A' might store processor data, location 'B' might store producer data, and location 'C' might store consumer data. Each site is self-sustaining, and is responsible for the applications that run on their site's servers. The advantage of a distributed system is scalability; up-scaling the system is easier because the sites are spread over several locations.

There are a number of issues which make the distributed system (Figure 1) more difficult to implement. One of them is data backup. Under a distributed system, each site defines its own backup policy. So some locations may backup data at regular intervals, while others may backup data irregularly or not at all. Another issue is the degree of external access, since each site will control its own security mechanisms protecting the database from outside access. Because each site may have their own policies, accessing information across multiple sites may be challenging. A third concern is the database security, both physical and digital. One location may use a simple password protection mechanism, while another site may use an advanced data encryption protocol. This is a concern for overall security, because the cyber security of any computer system is only as strong as its weakest link. For example, an attacker could launch an attack on the weakest site and once they accessed that site the attackers could use that site to launch attacks on the other potentially better protected databases sites. The fourth problem with distributed database systems is inter-site communications. Maintaining an up-to-date information registry across these multiple sites is difficult due to the increased communication overhead of transferring data back and forth. Tracing a particular product may require different sites to communicate with each other and a secure, inter-site communications protocol is required.

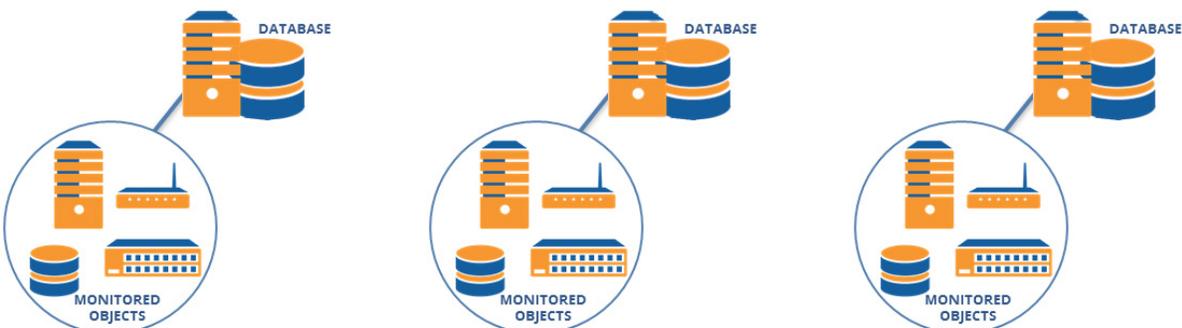


Figure 1. Structure of a distributed database system. Data is stored across multiple smaller databases. Each database may store information specific to one supply chain entity, such as processors or cow/calf operators. <https://www.sevone.com>

In a centralized or data silo database structure (Figure 2), all the data is stored in one location under one central command. For security purposes the centralized database would be replicated at other sites, so if a security breach (physical or cyber) happens, the centralized database at one of the alternate locations would become the primary system to maintain customer access. In a centralized database structure, many of the problems associated with a distributed system are no longer applicable. Policies can be defined according to a single standard, communication and data access is simplified, and security measures can be enhanced. There is also no need for inter-site communication protocols because there is no such communication; the database is self-contained in a single system. The primary weakness of a centralized system is that all the information is in one location and may be compromised if an attacker gains access.

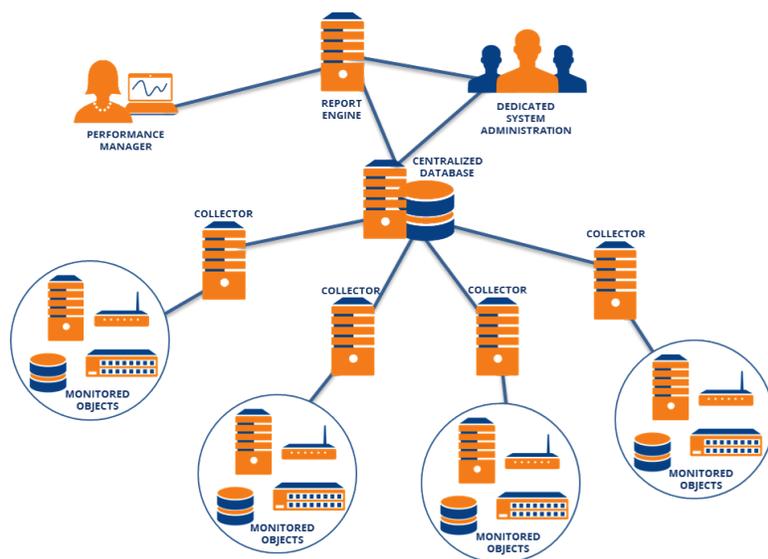


Figure 2. Structure of a centralized database system. All data is stored in one location where it is monitored by data administrators. <https://www.sevone.com>

Lastly is the issue of trust in the data administrator(s). Each site will have an administrator who has access to all the information in the system. This is necessary and essential because if there is a problem, the administrator can access the database, identify the problem, and correct it. An untrustworthy administrator could take advantage of their position to sell information, make malicious modifications, or delete data. This makes it essential that the data administrator(s) be a trusted third party, with no ties to any entity in the beef cattle supply chain.

For more information about the NWCTI system, contact Dr. Michael Buser using the information below. YouTube videos related to the NWCTI system can be viewed at <https://goo.gl/MwPhoS>.



THE SAMUEL ROBERTS
NOBLE
FOUNDATION

U of A
DIVISION OF AGRICULTURE
RESEARCH & EXTENSION
University of Arkansas System



This is a publication of the
National Whole Chain Traceability Institute.
Funding Agency: USDA National Integrated Food Safety
Initiative – Project Agreement No. 2011-51110-31044

Collaborators include the Oklahoma State University Departments of Agricultural Economics, Biosystems and Agricultural Engineering, Computer Science, and the Food and Agricultural Products Center; the Samuel Roberts Noble Foundation; University of Arkansas, Dale Bumpers College of Agriculture, Food & Life Sciences – Food Science; Top10 Produce.

Visit <http://nwcti.okstate.edu/> for more information or contact:
Dr. Michael Buser, Associate Professor
113 Agriculture Hall,
Stillwater, OK 74078
buser@okstate.edu

Oklahoma State University, in compliance with Title VI and VII of the Civil Rights Act of 1964, Executive Order 11246 as amended, and Title IX of the Education Amendments of 1972 (Higher Education Act), the Americans with Disabilities Act of 1990, and other federal and state laws and regulations, does not discriminate on the basis of race, color, national origin, genetic information, sex, age, sexual orientation, gender identity, religion, disability, or status as a veteran, in any of its policies, practices or procedures. This provision includes, but is not limited to admissions, employment, financial aid, and educational services. The Director of Equal Opportunity, 408 Whitehurst, OSU, Stillwater, OK 74078-1035; Phone 405-744-5371; email: eeo@okstate.edu has been designated to handle inquiries regarding non-discrimination policies; Director of Equal Opportunity. Any person (student, faculty, or staff) who believes that discriminatory practices have been engaged in based on gender may discuss his or her concerns and file informal or formal complaints of possible violations of Title IX with OSU's Title IX Coordinator 405-744-9154. Issued in furtherance of Cooperative Extension work, acts of May 8 and June 30, 1914, in cooperation with the U.S. Department of Agriculture, Director of Oklahoma Cooperative Extension Service, Oklahoma State University, Stillwater, Oklahoma. This publication is printed and issued by Oklahoma State University as authorized by the Vice President, Dean, and Director of the Division of Agricultural Sciences and Natural Resources and has been prepared and distributed at a cost of 20 cents per copy.