Data Driven Quantitative Trust Model for the Internet of Agricultural Things

Weili Han[1,3,4], Yun Gu[1], Yin Zhang[1], and Lirong Zheng[2]
1. Software School, Fudan University, Shanghai, 201203
2. School of Information Science and Engineering, Fudan University, Shanghai 200433
3. Shanghai Key Laboratory of Data Science, Fudan University, Shanghai, 200433
4. DNSLAB, China Internet Network Information Center, Beijing 100190

***Abstract*—With frequent food safety incidents, it becomes urgent and important to design an intuitively quantitative trust model to describe the trustworthiness of foods delivered in supply chains. However, current existing models are usually too subjective, because they heavily depend on experts' experiences to model the trust and set relevant parameters. Fortunately, the Internet of Agricultural Things may offer a big volume of business data, including product information and delivery information etc., via its pervasive sensing. These data motivate us to design a data driven quantitative model to evaluate the trust of sensed products in supply chains. The proposed trust model leverages a Bayesian network, where almost all parameters are set by the data rather than experts' experiences, to evaluate the trust value of a target product. Finally, a case of pork product is used to show the effectiveness of our trust model. Based on the comparison with other models, our model is promising to reduce the subjectivity and time-delay of the trust evaluation.**

Keywords- Internet of Things, Quantitative Trust Model; Data Driven; AIoT

I. INTRODUCTION

Food safety is a serious challenge because continuous food accidents, such as "2008 Chinese milk scandal" [6], occurred one after another recently. Various countermeasures have been taken in attempt to solve the food safety problem [4]. The Internet of Agricultural Things (AIoT), where the technologies of the Internet of Things are widely used in all of the phases in the agriculture industry, is proposed to resolve the food safety problem [14]. However, the technologies of AIoT cannot tell whether the food is trustworthy, though they can be good at displaying the processes of food production, transportation, etc. When a customer wants to buy an agricultural product, a simple and linear indictor, such as trust or reputation, can help the customer make decision. Otherwise, when a customer is surrounded with a flood of product information, including locations, shelf life, factories and other information about the product, it is hard for the customer who lacks professional knowledge to judge whether the product is trustworthy. Thus, it becomes highly necessary to find a solution to judge the trustworthiness of a product in AIoT.

Trust models are a good choice to judge trustworthiness. However, current trust models [2, 5, 7] heavily depend on experts' experiences during trust evaluation. In these models, the experts might subjectively set the parameters, and then make an error-prone trust evaluation. In addition, the parameters cannot be justified in time according to the daedal applications in the Internet of Things. Then the evaluation might be delayed to the real situation. For example, when the emerging cooling transportation technology can extend the food expiration, the parameters must be justified. But experts might not respond to this point, and give a misleading evaluation.

We, therefore, proposed a data driven quantitative trust model, where sensed and accumulated data in AIoT are leveraged to set the concrete parameters in our proposed evaluation model. The model takes selected factors into account when a system evaluates the trust. The information needed in evaluating these factors is based on historical data rather than experts' experiences. After the values' of these factors are obtained, they will be combined through a Bayesian network to calculate a quantitative trust value.

Furthermore, in order to explain the trust model in detail and show its advantages of application in AIoT, we provide an application of our trust model in countering the food safety problem. In the application, we calculate the quantitative trust value based on six factors. And finally we use a case of pork products to exemplify the application.

The main contributions of this paper are as follows:

- We propose a data driven quantitative trust model for AIoT. In this model, a big volume of sensed data rather than experts' experiences play an important role. The parameters in the trust evaluation can be set according to the real situation. Thus, the model is more neutral, and can tell the difference between products in the same supply chain.
- Real-time factors (time, location, signature validation) are taken into account when we evaluate the trust of products in AIoT. As a result, the proposed trust model can provide more timely results to users.

The rest of this paper is organized as follows: Section II investigates the related work and compares our trust model with others. Section III introduces our data driven quantitative trust model. Section IV introduces the application of the trust model in AIoT. Section V uses a case about pork products to exemplify the trust model. Section VI introduces the prototype of our model. Section VII discusses some important issues and challenges our model faces with. Section VIII concludes the paper and proposes our future work.

II. RELATED WORK

To the best of our knowledge, there is still no trust models designed for the food safety in IoT. However, there is some trust models designed for IoT, but they have some flaws to evaluate the trust of the products in AIoT. We compare our model with those trust models in Table I.

Dong et al. proposed a trust model for the IoT called TRM-IOT [3]. This model uses reputation as the main index of trust, which means each node's trust value comes from others' rating. However, if we only use the company reputation as the index of trust evaluation, the result would be not correct and timely. Li et al. proposed a multi-dimensional trust evaluation model for large-scale P2P computing [13]. This model uses WMA-OWA to combine several factors to evaluate the trust. But the factors include assumptions, expectations, behaviors, etc., which partly depend on experts. Because data in AIoT are too massive for experts to judge, Li's model is not suitable to

be applied to evaluating the trust of products in AIoT. Hexmoor et al. proposed a trust-based security model [1], in which entities' trust is evaluated to keep the security. But the model's trust evaluation needs behavior data and experts' experiences. This is unsuitable in evaluating products of AIoT. Wang et al. proposed a topology transform-based recommendation trust model which can relieve the malicious effects on the accuracy of recommendation trust [10]. But their model still uses recommendation so that it requires other's to make comments. However, recommendation is unsuitable in AIoT.

TABLE I. FEATURES OF CURRENT TRUST MODELS AND RESEARCHES IN FOOD SAFETY

	Independence of expert knowledge	Quantitative	Product data-driven	Can evaluate the trust of product	Take real-time factors into account
Our model	√	√	√	√	√
Li et al.'s model [13]		√	√	√	
TRM-IOT [3]	√	√		√	
Hexmoor et al.'s model [1]		√		√	
Wang et al.'s model [10]	√	√		√	
Shi et al.'s model [9]	√	√		√	

*Note: Product data driven means the data source only depends on the product data, rather than recommendation or third part rating.

Some other researches study the trust of food safety, but they focus on what have influences on consumers' food safety opinions [8] and build trust model to evaluate the factors on customer's buying behavior [11]. Shi et al. proposed a trust model that assists users and machines with decision-making in online interactions by using past behavior as a predictor of likely future behavior [9]. The model can automatically compute trust based on self-experience and the recommendations of others. But behavior-based (or experience-based) models are not suitable for evaluating products' trust because some features of products are unique (such as production time). There is still no trust model which aims to calculate the trust value of a product by collecting massive data (both historical data and real-time data) and evaluating them.

III. DATA DRIVEN QUANTITATIVE TRUST MODEL

We present a data driven quantitative trust model as follows:

Step 1 **Identify the impact factors.** As long as a factor has influence to the trustworthiness of the evaluated product, it should be considered as an impact factor. Besides, factors can be divided into groups by their common features.

Step 2 **Calculate the value of each factor.** After we identify impact factors, we need to use functions to calculate their values. Each factor's value is in the range of [0, 1]. The functions to calculate the factors may be different. We will use weight average and sigmoid functions in later applications (Section IV). To use weight average and sigmoid functions can help to adjust the influence of different factors in the result of the trust model. Note that, other functions are also applicable in our model.

Step 3 **Use a Bayesian network to combine the factors to evaluate the trust value.** A Bayesian network is used to combine the factors and calculate the final quantitative trust of the product.

We choose to use data driven method in our model because of the following reasons:

- In AIoT, we can obtain massive and reliable data. With adequate and reliable data, data driven trust models can work well. In AIoT, reliable data mainly include historical data (production time, locations, shelf life, et al.) and certificates (E.g., ranks awarded by governmental agencies).
- Trust evaluation can work more efficiently by data driven methods than by experts. Because, data used in data driven models are historical data and certificates, they usually stored in database which can be obtained quickly. In addition, the process to calculate the trust value by these data is simple and quick. So the whole data driven trust evaluation can work efficiently, which meets the requirements of AIoT which contains massive data which need to be handled in time.
- We do not use rating or recommendation in our trust model because both of them require other entities in the system to comment on the product. But in AIoT, a product is always disposable, which means it is impossible for our entities to rate or make recommendation to each other.
- We do not solely depend on expert knowledge in our trust model because experts might not deal with the requirements of the neutral and timely trust evaluation in AIoT.

IV. QUANTITATIVE TRUST EVALUATION IN AIOT

A. Factors in Trust Evaluation

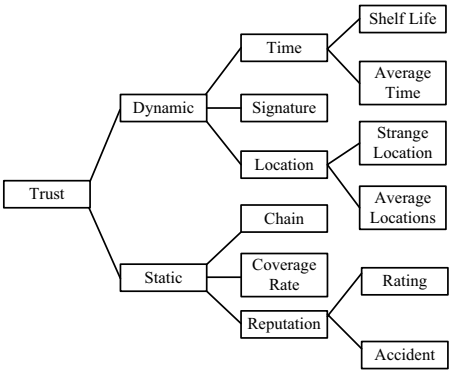

Figure 1. Factors in the trust evaluation

Figure 1 shows factors need to be taken into account in the trust evaluation in AIoT. Note that, these factors are proposed according to our investigation on the supplies of agricultural products. In addition, we leverage the data driven method to reduce the subjectivity in parameter setting.

According to the frequency of value change, all impact factors are divided into dynamic factors and static factors.

1) Dynamic Factors

Dynamic factors are those factors whose value changes frequently. Those dynamic factors need to be evaluated for every product.

a) Time

Shelf Life: All products have shelf life. Once the time exceeds the shelf time of a product, the product is considered as useless and untrustworthy.

Average Time: It is not enough to estimate the time factor in trust evaluation only by shelf life. Because two products will get same trust value as long as they are both in their shelf life. However, there certainly exists difference when one of them was produced 7 days ago and the other was produced 20 days ago. Therefore, we introduce the concept called average

time to estimate time factor in addition to shelf life. The average time is the average time a product of a kind spends on a shelf. We calculate the average time used for a type of food. Then, we use this average time as a standard to compare the trustworthiness of products in the same type.

b) Location

Strange Location: Same type of food, especially those produced by same factories in the same supply chain, often appears in the same location because the origins of a type of product are centralized and transportation routes are similar. Besides, products in the same batch should have same track. If one of them appears in a strange location, then it seems to be untrustworthy.

Average Locations: The number of the locations products reached also needs to be taken into account in trust evaluation. Therefore, we introduce the concept called average locations. We calculate the average number of locations reached for a type of products. Then we use the value of average locations to help generate the trustworthiness of products in the same type.

c) Signature

In electronic pedigree systems [4][15], we use digital signatures to ensure the integrity of the whole system. Companies who sign on the electronic pedigrees are responsible for the information they provided with their signatures. However, some signatures in the electronic pedigree may be invalid, caused by counterfeiting and information changes. So we need to check the validity of signatures on the product to evaluate its trustworthiness.

2) Static Factors

Static elements are those elements whose value rarely changes. Static factors can be evaluated only once for a quantity of products.

a) Chain

In a food supply chain, there are many companies who are in charge of different processes. In general, the food supply chain includes production, processing, inspection, transportation, storage and sale. We regard each company in the supply chain as a node. The more nodes a food supply chain has, the less trustworthy it is. Because more nodes mean that more participants are involved in the supply chain, more middlemen will bring out higher risks of accidents.

b) Coverage Rate

The electronic pedigree systems for AIoT recommend that all processes in the food supply chain use electronic pedigrees to keep the integrity of the system. However, it is unavoidable that some processes are not covered with electronic pedigree protection. So we have to take the coverage rate of electronic pedigree into account when we evaluate trust.

c) Reputation

The reputation for a company represents the confidence of public for its product. Reputation is also an important factor in trust evaluation. We only consider two objective factors, rating and accident rate in the trust evaluation.

Rating: Rating often comes from the opinions of former consumers. But in AIoT, consumers are not asked to give scores to the products they bought as online shopping systems. So we estimate this factor by official data. Most companies have a rank offered by governmental agencies. It can be taken into account during the trust evaluation.

Accident: Food accidents happened frequently these years. If an accident happens in a food supply chain, the trust of products in this chain will certainly be influenced. In addition, the time of the accident is also meaningful.

B. Evaluation Functions of Factors

1) Time

Shelf Life (t_{shelf}) is set by the producer of the product. It has only two values. 0 means the product has exceeded shelf life. 1 means the product is within its shelf life.

Average Time is calculated by comparing the time used of the product with the average time span for the same type of products. First, we calculate the *Average Time* span for products belonging to the same type of the evaluated product.

Then use equation (1) to get $t_{averagetime}$. t is the time used by the evaluated product.

$$t_{averagetime} = \begin{cases} \frac{1}{1+e^{6-\frac{12\times Average\ Time}{t}}} & t > Average\ Time \\ 1 & t \le Average\ Time \end{cases} \quad (1)$$

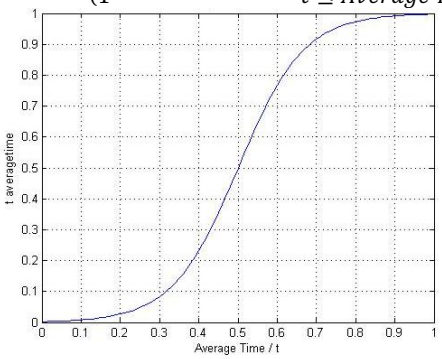

Figure 2. A modified sigmoid function whose independent variable and dependent variable are both in the range of [0, 1]

We use a sigmoid function as showed in Figure 2 to express the relationship between $\frac{Average\ Time}{t}$ and $t_{averagetime}$. With the decrease of t, $\frac{Average\ Time}{t}$ will increase and $t_{averagetime}$ will increase as well.

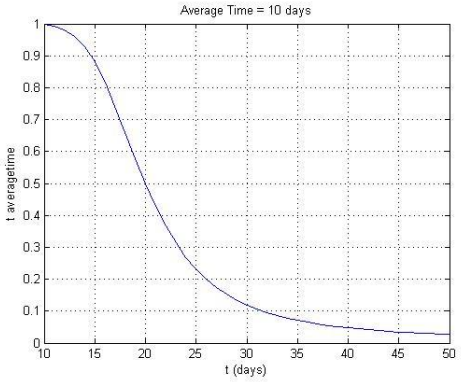

Figure 3. $t_{averagetime}$ evaluation when *Average Time* = 10 days

In order to better illustrate the relation between $t_{averagetime}$ and t, we take *Average Time* = 10 days as an example. Figure 3 illustrates the relation between the time of the product (t) and the trust value get from average time factor ($t_{averagetime}$) when the average time for this kind of product is 10 days. With the time passing, the trust value is smaller. In addition, the trust value decreases gently within 15 days, steeply from day 15 to day 25, and then gently again after day 25. The result is in accordance with the actual case.

The trust estimated from shelf life (t_{shelf}) and average time ($t_{averagetime}$) is combined by multiplication as showed in equation (2).

$$t_t = t_{shelf} \times t_{averagetime} \quad (2)$$

2) Location

Strange Location is judged by elimination. The set of valid cities for a certain kind of products will be given by

investigating the locations reached by most products of the same type. Any unlisted location is regarded as a strange location. There are only two values (0 and 1) of $t_{strange}$. 0 means that there exists a strange location. 1 means that all locations the product reached are valid.

Average Locations is calculated by comparing the number of locations the evaluated product reached with the average number of locations reached by same type of products. First, we calculate the *Average Locations* for the products belonging to the same type of the evaluated product. Then, we use equation (3) to get $t_{averagelocation}$. lo is the number of locations reached by the evaluated product.

$$t_{averagelocation} = \begin{cases} \frac{1}{1+e^{6-\frac{12\times Average\ Locations}{lo}}} & lo > Average\ Locations \\ 1 & lo \le Average\ Locations \end{cases} \quad (3)$$

The trust estimated from strange location ($t_{strange}$) and average locations ($t_{averagelocation}$) are combined by multiplication as shown in equation (4).

$$t_l = t_{strange} \times t_{averagelocation} \quad (4)$$

3) Signature

We use the proportion of valid signature to evaluate t_s.

$$t_s = \frac{Valid\ Signatures}{Valid\ Signatures+Invalid\ Signatures} \quad (5)$$

4) Chain

The evaluation of trust according to the number of nodes in chain is similar to that of $t_{averagetime}$ and $t_{averagelocation}$. The suitable number of nodes varies for different type of food. So we use *Average Nodes* in a certain field as a reference standard. First, we calculate *Average Nodes* (average number of the nodes) of the products belonging to the same type of the evaluated product. Then we use equation (6) to estimate t_n. n is the number of nodes in the chain of the evaluated product.

$$t_n = \begin{cases} \frac{1}{1+e^{6-\frac{12*Average\ Nodes}{n}}} & n > Average\ Nodes \\ 1 & n \le Average\ Nodes \end{cases} \quad (6)$$

5) Coverage

As common sense, the higher the coverage rate is, the more trustworthy the products are. The best case is that all processes are covered with electronic pedigrees ($t_c = 1$) while the worst case is that no process is covered ($t_c = 0$). We use equation (7) to estimate t_c.

$$t_c = \frac{Process\ with\ Pedigrees}{Number\ of\ Processes} \quad (7)$$

6) Reputation

Rating can be gotten from the company's certificates or the governmental agencies. Most companies in the market are ranked by professional rating organizations. They are usually ranked from AAA to C. The rank corresponds to different value of t_{rank} as shown in Table II. If the official rating of the product is lacking, we use a default value. Usually, the default value is the average rating of the field. After each company's rank is translated into a number through Table II, we use the average rank of all the companies involved in the evaluated product's supply chain as the value of t_{rating}.

Accident rate can be offered by the company itself as well as from supervision of government. $t_{accident}$ can be calculated by equation (8).

$$t_{accident} = w_1 \times a_1 + w_2 \times a_2 + \cdots w_n \times a_n \quad (8)$$

a_1, a_2 .... a_n are accident rates in the past N years, and w_1, w_2, ... w_n are their weight.

The trust estimated from rating (t_{rating}) and accident rate ($t_{accident}$) will be combined by multiplication as showed in equation (9).

$$t_r = t_{rating} \times t_{accident} \quad (9)$$

TABLE II. RELATION BETWEEN RANK AND t_{rank}

Rank	t_{rank}	Rank	t_{rank}
AAA	1	BBB	0.5
AA	0.9	BB	0.3
A	0.7	B	0.1
C or Below	0	-	-

C. Trust evaluation based on a Bayesian Network

We choose a Bayesian network to calculate the final trust value considering all these factors. Bayesian network is a mathematic tool which is able to maintain the relations between various factors and adjust the weight of factors easily by change the probability.

Figure 4 is an instance of Bayesian network for our trust model. All nodes in the Bayesian network has two possible values, T (for trustworthy) and F (for untrustworthy). Each node has a table to show its T and F probability under different conditions.

We get the value of t_t, t_l, t_s, t_n, t_c and t_r by functions introduced in Section III.B. We then calculate the values of the dynamic factors t_d and static factors t_s. At last, we calculate the quantitative trust value.

V. A CASE STUDY IN AIOT

In this section, we will show the trust evaluation process of our trust model with an example of two products in pork production.

First, we get the following information from historical data.

- *Average Time* = 10 days
- *Average Locations* = 5
- *General Location* = {Shanghai, Nanjing, Changzhou, Hangzhou, Ningbo}
- *Average Nodes* = 6
- Weights of accident rate for last three years: 0.5, 0.3, 0.2

Second, we calculate the trust value for each product. Here we list two products, which are product A and product B. Figure 5 shows the information of the product A and B. We can get this information from electronic pedigrees systems and other information systems of companies related to the products.

From the left part of Figure 5, we can get the information of product A as following:

- *Shelf life* = 50 days
- *t* = 12 days
- *Locations* = {Shanghai, Hangzhou, Changzhou, Nanjing}
- *n* = 6
- *Coverage rate* = 1
- *Ranks* = {AAA, AA, AAA, BBB, AA, AAA}
- *Accident rate* = {0.98, 0.98, 0.95}

Then, we can calculate the six factors' values.

(1) The product is in its shelf life (12 < 50), so $t_{shelf} = 1$.
Average Time = 10 days, *t* = 12 days, so
$t_{averagetime} = \frac{1}{1+e^{6-12\times\frac{Average\ Time}{t}}} = \frac{1}{1+e^{6-12\times\frac{10}{12}}} = 0.982$,
$t_t = t_{shelf} \times t_{averagetime} = 1 \times 0.982 = 0.982$

(2) There is no strange location, so $t_{strange} = 1$
Average Locations = 5 cities, $lo = 4$,
$lo < Average\ Location$, so $t_{averagelocation} = 1$
$t_l = t_{strange} \times t_{averagelocation} = 1$

(3) Valid Signatures = 6, Invalid Signatures = 0,
So $t_s = \frac{Valid\ Signatures}{Valid\ Signatures+Invalid\ Signatures} = \frac{6}{6+0} = 1$.

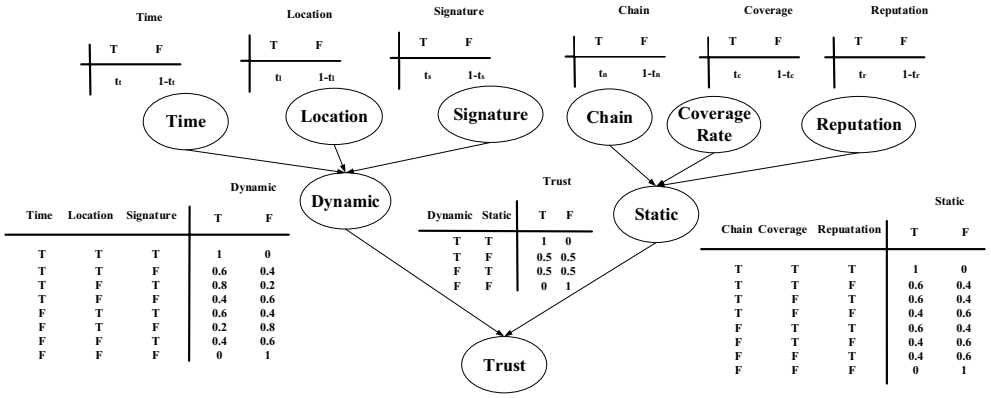

Figure 4. Bayesian network for trust model

(4) *Average Node* = 6 nodes, $n = 6$ nodes, so $t_n = 1$

(5) There are 6 nodes in the food supply chain and all are covered with electronic pedigree, so $t_c = 1$

(6) The ranks of the companies in the supply chain are {AAA, AA, AAA, BBB, AA, AAA}, so their value is {1, 0.9, 1, 0.5, 0.9, 1}.

$t_{rating} = \text{avg}(\{1, 0.9, 1, 0.5, 0.9, 1\}) = 0.883$

Past three years accident rate = {0.98, 0.98, 0.95}

$t_{accident} = 0.5 \times 0.98 + 0.3 \times 0.98 + 0.2 \times 0.95 = 0.9740$

$t_r = t_{rank} \times t_{accident} = 0.8833 \times 0.9740 = 0.8603$

Next, we get $t_d = 0.982 * 1 * 1 + 0.018 * 1 * 1 * 0.6 = 0.9928$ and $t_s = 1 * 1 * 0.8603 + 1 * 1 * 0.1397 * 0.6 = 0.9441$.

At last, we get the trust value of product A: $trust_A = 0.9928 * 0.9441 * 1 + 0.0072 * 0.9441 * 0.5 + 0.9928 * 0.0559 * 0.5 = 0.9685$

Similarly, we get the trust value of product B: $trust_B = 0.6381$.

Compare the results of trust evaluation of product A and product B, we get that $trust_A > trust_B$. So product A is more trustworthy than product B.

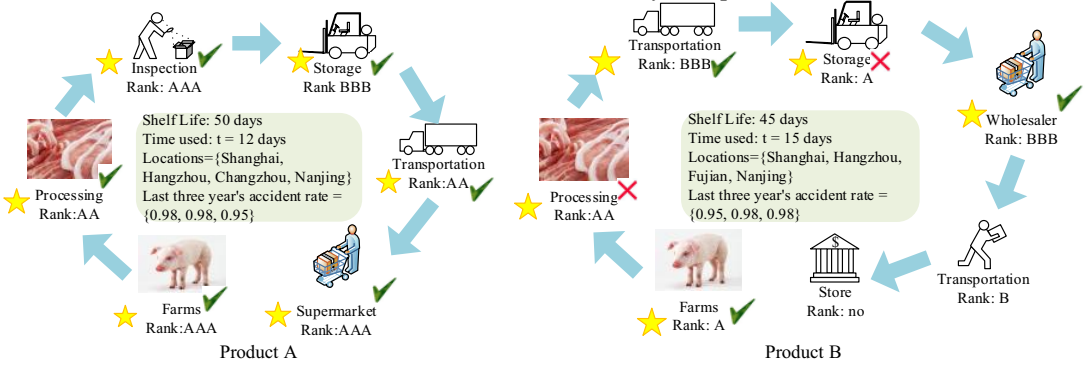

Figure 5. Case study for our proposed data driven quantitative trust model

VI. PROTOTYPE

We apply the trust model to AIoT with the support of an electronic pedigree system [4][15]. According to Section III.B, we need to calculate the value of six factors (time, location, signature, chain, coverage and reputation). As is shown in Table III, the data needed mainly come from two sources, which are electronic pedigrees [EP] and reference database [RD]. A product may obtain these electronic pedigrees from electronic pedigree systems [4]. Furthermore, EPCIS can provide the data sources for reference data.

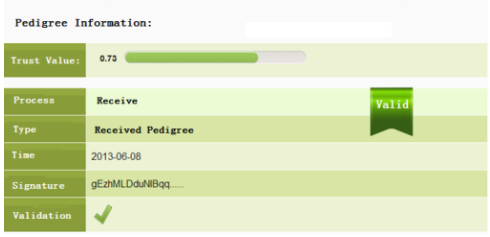

Figure 6. Electronic pedigree with trust value

We built up the prototype in AIoT. Figure 6 shows the electronic pedigree page of a product which includes the trust value of the product.

TABLE III. INFORMATION NEED TO GET WHEN CALCULATES IMPACT FACTORS

Factor		Information
Time	*Shelf Life*	Current Time , Production Time [EP]
	Average Time	Current Time, Average Time [RD]
Location	*Strange Location*	Locations [EP], Safe Location List [RD]
	Average Locations	Location number [EP], Average Locations [RD]
Signature		Valid Signature [EP], Invalid Signature [EP]
Chain		Node number [EP], Average Node [RD]
Coverage		Process with pedigree [EP], Total Processes [RD]
Reputation	*Rating*	Company rating [RD]
	Accident	Accident Rate [RD]

VII. DISCUSSION

As we mentioned above, our trust model is based on historical data and facts. These data can be obtained from the products themselves, related companies and the governmental agencies. Take a piece of pork as an example. We can find the ID on the surface of the product. We then use the ID to find the electronic pedigrees of this piece of pork from the Internet. Locations, time, person in charge, companies' names and other information will be recorded in these electronic pedigrees. Besides, we can know the rank of these related companies with the help of the governmental agencies.

To ensure the trustworthiness of the data used to calculate factors, we should have some measure to ensure the data quality. We must guarantee the data providers are responsible for the data they provide. Using electronic pedigrees in the production of products will be useful in meeting this requirement. Any company or person who wants to add some information to the product is required to sign the digital signatures. In addition, deleting or modifying data are forbidden because they will badly break the trustworthiness of data.

In the Bayesian network of our trust model, middle nodes (dynamic and static nodes in Figure 4) can be determined according to the concrete application scenario. We leverage the concept of middle nodes because some factors can be divided into groups. These factors have similar influences on the trust and these influences can be simply adjusted by changing the probability of the group factor. For example, if we find the dynamic factors' influence on the trust of product is greater than that of static ones, we can just adjust the probability table of the dynamic node.

In addition, the probability table we used in the Bayesian network of the food safety application depends on our experience. Although the network works well in the motivated case, we can use the self-adaptive technology [12] to automatically justify these probabilities when the calculation offsets our expectation. For example, customers think some products' trust value should be lower or higher, the system can dynamically adjust the possibility table in the Bayesian network to make some factors more influential or less so.

VIII. CONCLUSION AND FUTURE WORK

We propose a data driven quantitative trust model, which is suitable to provide timely, neutral and quantitative trust evaluation of foods in AIoT. The model takes several objective factors into account and almost all the parameters used to calculate the factors are based on historical data or facts. A Bayesian network is used to combine the factors and evaluate the final trust of the product.

Compared with other trust models, our model is independent of expert knowledge. Besides, unlike rating or third-party recommendation models, the products in our model do not need interactions with other parties. These features help our model to meet the requirement of the trust evaluation in AIoT. In addition, our model not only considers static factors such as reputation but also real-time factors, such as time and location. This offers the trust value to tell the difference between products in the same supply chain, which is meaningful in real life.

Our future work will reduce the dependence on the experts' experiences, such as, to automatically identify the factors based on the business data. In addition, data veracity could negatively affect our model. Thus, how to clean the data before evaluation, even consider the dirtied data in during the evaluation could be our big challenges. Furthermore, we will bring out a viable mathematical proof on the value-addition and viability of this newly conceptualized trust model in the next period of the research.

ACKNOWLEDGEMENT

This paper is supported by the projects funded by 12th Five-Year National Development Foundation for Cryptography (MMJJ201301008), CNNIC DNSLab (Opening Project), Natural Science Foundation of Shanghai (12ZR1402600). We thank all anonymous reviewers for their comments. Weili Han is the corresponding author.

REFERENCES

[1] H. Hexmoor, S. Wilso, Sandeep Bhattaram, A theoretical inter-organizational trust-based security model, The Knowledge Engineering Review, 2006, pp.127-161.

[2] Z. Liu, A.W. Joy, R.A. Thompson, A dynamic trust model for mobile ad hoc networks, Distributed Computing Systems, 2004, pp. 80-85.

[3] D. Chen, G. Chang et al, TRM-IoT: A trust management model based on fuzzy reputation for internet of things, Computer Science and Information Systems, Volume 8, Issue 4, 2011,pp.1207-1228.

[4] W. Han, Y. Gu, W. Wang, Y. Zhang, Y. Yin, J. Wang, L Zheng, The design of an electronic pedigree system for food safety, Information Systems Frontiers, 2014, DOI: 10.1007/s10796-012-9372-y.

[5] Y.H. Tan, W. Thoen, Formal aspects of a generic model of trust for electronic commerce, Decision Support Systems, Volume 33, Issue 3, July 2002, pp. 233-246.

[6] Wikipedia, 2008 Chinese milk scandal, 2008.

[7] Y. H. Tan, W. Thoen, Toward a Generic Model of Trust for Electronic Commerce, International Journal of Electronic Commerce, Volume 5, Number 2 / Winter 2000 / 01, pp. 61-74.

[8] S.G. Sapp, S.R. Bird, The Effects of Social Trust on Consumer Perceptions of Food Safety, Social Behavior and Personality, 2003, 31 (4), pp. 413-421(9).

[9] J. Shi, G. Bochmann, C. Adams, A Trust Model with Statistical Foundation, Formal Aspects in Security and Trust, IFIP International Federation for Information Processing , 2005, vol 173, pp.145-158.

[10] K. Wang, M. Wu, Cooperative communications based on trust model for mobile ad hoc networks, Information Security, IET, Volume 4 , Issue 2, 2010, pp.68-79.

[11] A.E. Lobb, M. Mazzocchi, W.B. Traill, Modelling risk perception and trust in food safety information within the theory of planned behaviour, Food Quality and Preference, 2007, pp.384–395.

[12] P. Oreizy, M.M. Gorlick et al., An architecture-based approach to self-adaptive software, Intelligent Systems and their Applications, Volume 14, Issue 3, 1999, pp.54-62

[13] X. Li, F. Zhou, X. Yang, A multi-dimensional trust evaluation model for large-scale P2P computing, Journal of Parallel and Distributed Computing, 2011, pp.837-847.

[14] L. D. Xu, W. He, S. Li, Internet of things in industries: A survey in IEEE Transactions on Industrial Electronics, 2014, DOI: 10.1109/TII.2014.2300753.

[15] Y. Zhang, W. Han, W. Wang, C. Lei. Optimizing the Storage of Massive Electronic Pedigrees in HDFS, In Proceedings of IoT 2012, 2012, 68-75.