An Secure Information Security Provenance Model for Controlling Spurious Drugs in Distributed Environment

Arun .R[1], Balaji .P[2], Vinod .D[3]

[1, 2]Student, Department of Information Technology, Sri Ramanujar Engineering College, Anna university, Chennai - 600 127, India

[3]Professor, Department of Information Technology, Sri Ramanujar Engineering College, Anna university, Chennai - 600 127, India

Abstract: ***The objective of the work is to propose a distributed secure provenance system to gauge the trustworthiness of the drugs amidst spurious and counterfeit drugs. The distributed secure model has been implemented to share information provenance procedures in a health care industry. There are a number of Drug and Cosmetic Acts in the country for the control of illicit drugs, but more than 33% of the drugs are not genuine which necessitates a distributed provenance system with a high degree of data security. The secure provenance model addresses minimum loss of privacy of the pharmaceutical manufacturing companies so as to enhance the trustworthiness of the product and also the people. The model is implemented as a mobile deployment model with secured provenance against possible attacks.***

1. Introduction

It is apparent that drugs play the most imperative task in saving lives, restoring health, preventing diseases and epidemics. The World Health Organization (WHO) points out that 35% of spurious drugs in the world are from India. The delusive drug might turn the addictive menace to the patient and these spurious drugs do not remain native to their country but are also exported or smuggled. The significant Acts are implemented for the control on import, licensing and inspections (import and manufacture), rules for labeling, packaging, and storage, penal provisions of the act and rules (prosecutions, confiscations, suspension and cancellation) include the Drugs and Cosmetics (Amendment) Act, 1964, the Consumer Protection Act, 1986, Feeding Bottles and Infant Foods Act, 1992, etc. [1]. But still spurious drugs are delimited in our daily life. As increasing amounts of valuable information are produced and persist digitally, the ability to determine the origin of data becomes important [2]. In medicine data provenance tracking is essential for authentication of information as it flows through workplace tasks. While significant research has been conducted in this area, the associated security and privacy issues have not been explored, leaving provenance information vulnerable to illicit alteration. Trust is a particular value of subjective probability with which a member determines another member's behaviour or performance of a particular action in a particular context [3]. But in some scenarios when there are no frequent interactions between the entities, the trust value of an entity may tend to remain the same. Also, it does not consider the suspicion values for the entities. All the earlier trust models addressed the issue of context-dependency of trust during interactions, but did not incorporate the logic or mechanisms to evaluate trust by accounting the suspicion levels the trust actors might be subjected to. The context implies how and why the members trust the information that is given to them [4] In case of Trust Management systems the permission or authorization problem is expressed in terms of finding a proof of a particular formula representing successful interaction, with collection of suitable logic [5]. A trust model is a collection of rules that helps to decide the legitimacy of trust attributes or trust certificates. Trust is not only subjective, but also context dependent because the trust of one entity to another entity varies from one context to another. For a dynamic system, trust has to be predicted and managed efficiently along with consideration for trust levels in the future. The recommendation based trust model deals with the direct trust based on the reputation of the trustee which is given by a feedback. In this model, there are possibilities of deceptive recommendations which increase model's susceptibility to attack. In the evidential trust model [6] How to provide strong integrity and confidentiality assurances for data provenance information in the kernel, file system, or application layer is the problem. Now it is needed to have a secure provenance system for controlling spurious drugs in the market. It can be implemented by allowing customer to know the origin of the drug with minimum privacy loss of an organization. There are a number of IT standards and technology frameworks which are supporting organization independently. Information technology infrastructure library (ITIL) is the de-facto IT management framework and one of the most widely used IT standards[7].Here the standards of information security has been followed and extended in controlling organization framework. A key factor for achieving optimal security levels within supply chains is the management and sharing of cyber security information associated with specific metrics [11].

2. Distributed Provenance Model

Current model that automate the collection of provenance information use a centralized architecture for managing the resulting metadata - that is, provenance is gathered at remote hosts and submitted to a central provenance management service [4]. In contrast, we are developing a completely decentralized system with each computer maintaining the authoritative repository of the provenance gathered on it. Our model has several advantages, such as scaling to large amounts of metadata generation, providing low-latency access to provenance metadata about local data, avoiding the need for synchronization with a central service after operating while disconnected from the network, and letting users retain control over their data provenance records. It is needed to provide document evidence to the customers through a mobile service as and when the history of drugs are needed without affecting the privacy policy of the drug manufacturers to a larger extent in distributed environments, including how queries can be optimized with provenance sketches, pre-caching, and caching. Provenance may be specified on instances of an entity class and other provenance components are semantically related to various details about the events [8]. Trustworthiness in an inquiry is to keep up the claim that the findings are "worth paying attention to". The issues that require trustworthiness includes credibility, transferability, dependability and conformability. Credibility is checking of the research findings for considerable conceptual interpretation of the data taken from the volunteer's genuine data. Transferability is the extent to which the findings of this inquiry can be used for other projects. Dependability is a calculation of the quality of the data collection, data analysis and theory proposal. Conformability is the measure of how well the findings are supported by the data collected. In our paper, the trustworthiness is enhanced through the biological strategies.

2.1 Information risk analysis module

The information security governance module (ISG) indicates the objectives and operations about the security incidents that had happened or may happen inside or outside the organization. The focus of governance is to identify the various risk and security compliance (ISC) in different directions and dimensions so as to take decisions that defines the expectations to grant the regulation processes. The information security risk (ISR) analysis based on the business processes is configured, not only to regulate the processes but also report the necessary updates. The interfaces are modelled to track the information for various process to avoid the development of risk and non compliance. In such requirement the policy structure also defines the CIA to vary acceptable and non acceptable risk in a secure organization.

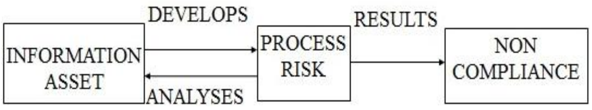


Figure 2: Interface 1: Interface (process risk & noncompliance)

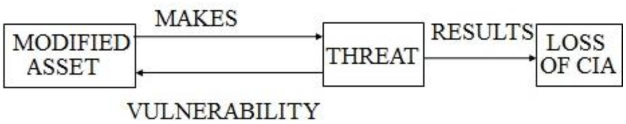


Figure 3: Interface 2: Interface (threat & CIA)

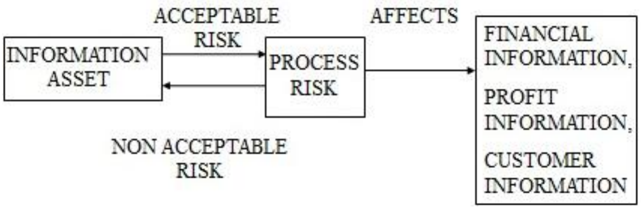


Figure 4: Interface 3: Interface (process risk)

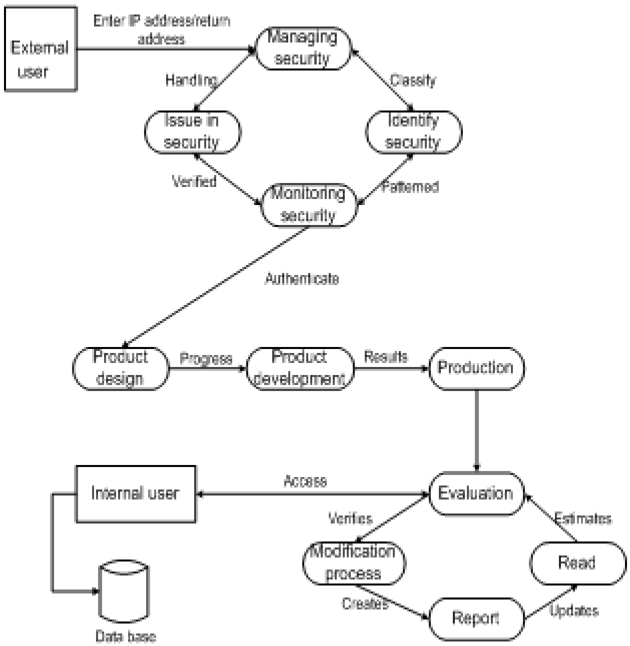


Figure 5: Information security process flow model

The interface process through information security assets has been implemented in various states to elaborate information processing check. In environment which develops process risk that results in non compliance in interface1fig 2 while it get processing the information should results in non compliance ,When the other interface process through modified asset which results threat and leads in confidentiality the weakness of the organizations data sources results in threat and it makes through the loss of CIA the integrity and authorization is done with in interface2 fig 3.The interface makes a sensible information assets in interface 3 fig 4 which brings non acceptable risk that leads in organisations information failure. In order to archive certain information assurance the information flow process has been adopted with external and internal process with monitoring product design. The evaluation and extraction of information can be regulated in information retrieval, where as managing the security issues with various security identity and authorization can be evaluated with authenticated security monitoring system, this procedures has been extracted in and formalized in Fig 6.This approach has been compared with the previous information processing and controlling procedure in World Health Organization focus on trust value of an entity and suspicion values for the entities .The approach have analysed in this work has overcome drawbacks and issues faced in the above discussed procedures.

3. Information Secure Spurious Drug Control Systems

The drugs details are stored electronically as digital documents. It contains information about drug such as Name of the company, Date of Manufacture, Expiry date, Composition, Quantity, Coating, License Number, Doctor name, Messaging. The aim of information security is to ensure business continuity and minimise business damage by preventing and minimizing the impact of security incidents [10]

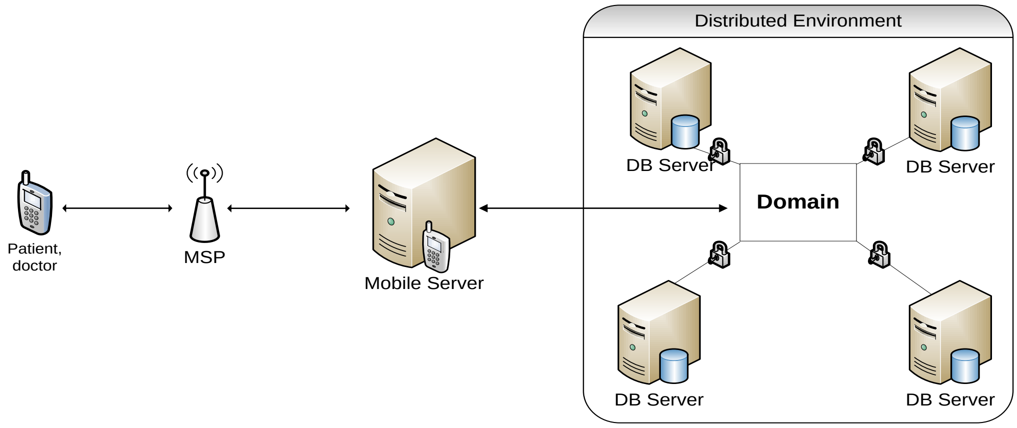


Figure 6: Domain access module

This information's are often accessed by buyer of the drugs. Information security and privacy in the healthcare sector is an issue of growing importance. The adoption of digital patient records, increased regulation, provider consolidation [12]. Adversary modification on this information may lead to problem of spurious drugs. In order to trust the accessed information about the drugs we need to know its provenance. Provenance system records the modification done on the drug details. This Spurious control system gets Drug name and Batch number as input from the patient or doctor. Mobile services provider and mobile server forward the input data to corresponding company database server. Input data are processed at virtual network and returns information generated from provenance record. The information contains details such as expiry date, drug is genuine or fake, manufacture date etc. patient, when he doubts about the quality of the drug, will make his enquiry through mobile with these details like name of drug, company name, license number, date of manufacture, expiry date, shop name, name of the doctor, etc. Once these set of data are verified and when found to be true the server returns the dosage, type of drug, prescription method, last inspected by the authority and supplier details from database. If the patient found these details unsatisfactory, he would be provided with the website details and complaint form. The mobile user can submit his query to know the history of the drugs and the service brings out the history or the status of the drugs through a federated web services as shown in figure 1.

4. Secure Provenance Model

In general, provenance collection mechanisms become harder to subvert when they are implemented at lower levels of a system. However, we can never track provenance perfectly, because a provenance tracking system implemented at a particular level of the system is oblivious to attacks that take place outside the view of that level. For example, suppose that we implement provenance tracking for tuples inside a database management system. An adversary can subvert provenance collection by opening the database file with a private copy of the database management system that has provenance collection turned off, or by using a file editor to modify the database file. Suppose instead that we implement provenance tracking in the OS kernel. If the kernel is not running on hardware that offers special security guarantees, an intruder can take over the machine, subvert the kernel, and circumvent the provenance system. Making a provenance record trustworthy is challenging. Ideally, we need to guarantee *completeness*—all relevant actions pertaining to a document are captured; *integrity*—adversaries cannot forge or alter provenance records; *availability*—auditors can verify the integrity of provenance information; *confidentiality*—only authorized parties should read provenance records as shown in fig 7; and *efficiency*—provenance mechanisms should have low overheads.

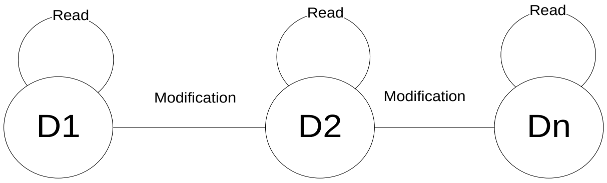


Figure 7: Secure provenance model
δ (D1, Read) => D1 , δ (D1, Modification) => D2

5. Information secure Suspicion Stack

The four different stacks based on the contexts are as follows: (i) Entity Information Suspicion (EIS) stack (ii) Task Suspicion (TS) stack (iii) Process Suspicion (PS) stack (iv) Attack Suspicion (AS) stack. The corresponding suspicion level in the respective suspicion stack is checked and then trust value is predicted. If the suspicion value of the stac k changes from high to low, then the trust value increases as if it changes from low to high, then the trust value decreases. In this manner, trust value can be predicted for any member. An instance of the suspicion stack in four contexts is illustrated in figure 8.

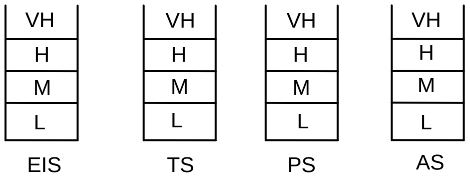


Figure 8: Various Information Suspicion Stacks

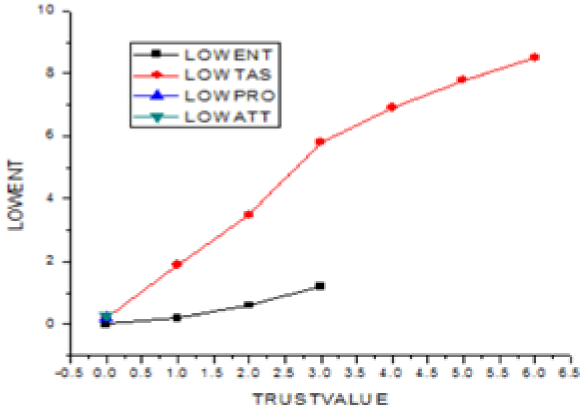
In the proposed model when an External Attack Context is considered, unreliable entities or tasks or processes can be eliminated. Also reputation has been given a significant role because the previous suspicion values for any context can be determined or made available using the suspicion stacks. At the lowest level of the trust model, the incoming items may be considered as the symbols on the tape of a Turing machine. As the details are passed through the input tape, the corresponding context suspicion stack is checked. Only if the top value of the stack is an acceptable value; trust is assigned to that member. Here it is processed to apply “Metrics are tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data.[9] in order to deal with suspicious trust value.

Table 1: Suspicion trust value

ENTITY	TASK	PROCESS	ATTTACK
L= 1-3	EL>=11	ETL≈21-23	ETPL<31
M=4-6	EM >=11	ETM≈21-26	ETPM<31
H=7-9	EH>=11	ETH≈21-29	ETPH<31
VH=10	EVH>=11	ETVH≈21-30	ETPVH<31

Here the (ETPA) entity, task, process and attack has been derived with equivalent values in low, medium, high and very high trust values assigned and verified with equivalent output. The entity has been specified with (L, M, H, VH) with a min of (1) and max value (10). The Task has been specified with (EL, EM, EH, EVH) with a max value of (11), The process specified with (ETL, ETM, ETH, ETVH) with a min of (21) and max value (30).

The attack specified with (EPTL, ETPM, ETPH, ETPVH) with a max value (31). The trust values have been calculated as per the low and very high value to a specific transaction through internal and external access in the above mentioned table 1. Hence low and medium trust values can be consider as trusted users with permit access on available asset.
L= Low
M=Medium
H=High
VH=Very High
EL=Entity low
EM=Entity medium
EH=Entity high
EVH=Entity very high
ETL=Entity task low
ETM= Entity task medium
ETH= Entity task high
ETVH= Entity task very high
ETPL= Entity task process low
ETPM= Entity task process medium
ETPH= Entity task process high
ETPVH= Entity task process very high



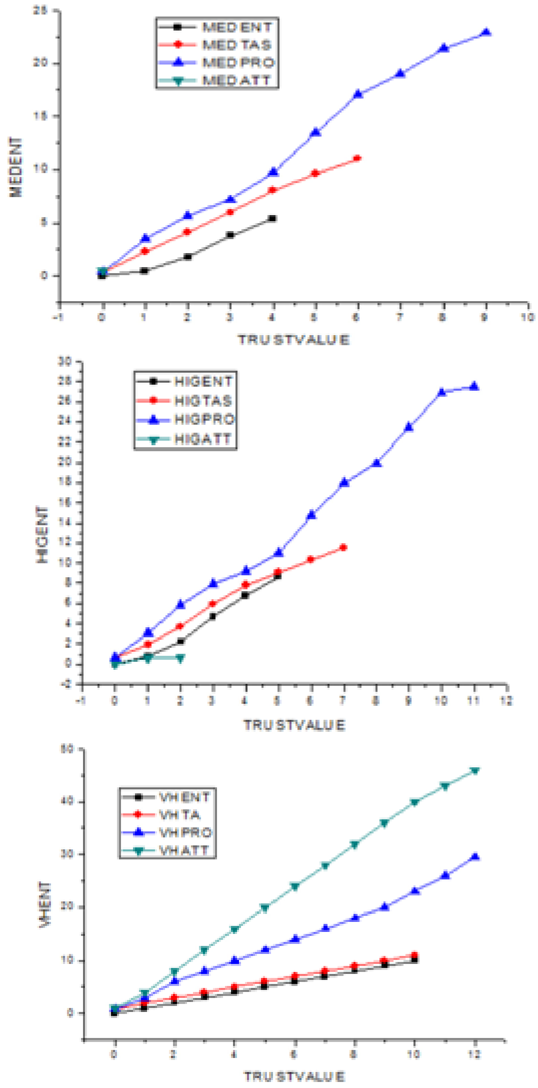


Figure 9: Low, Medium, High, Very High Graphical Results

Similarly, consider the trust level for a member to be Tij where i= {0, 1, 2} at a given context Cj and let the jth context’s stack top value to be ST. Let the only acceptable suspicion value on the top of the stack is L upon which the trust value can be assigned to an item and then allowed to move to the next trust level (Tj+1).
This implication can be represented as

(Tij, Cj, ST) →T(i+1)j, where j={e, t, p, a}; i={0,1,2}

Consider an input entity from an entity set {E} at the trust level T1e with the suspicion value at top of stack as VH (Very High), then its transition (δ), can be represented as
δ (T1j, {E}, VH) →(T0j, ε) where j={e, t, p, a}
When the Top value of the stack is VH, the stack top value is removed. This removing of the stack value is represented as ε.
The trust level of an entity decreases to T0j since it has a suspicion value of VH. For an entity {E} with the stack top appears to be at H(High),its transition can be represented as
δ (T1j, {E}, H) → (T0j, ε)

Similarly, for the entity from entity set {E} with the stack top value as M (Medium), the transition can be represented as

δ (T1j, {E}, M) →(T0j, ε)

When the entity enters, the suspicion stack is checked and if the stack top value is L (Low) which is the permissible value for a member,

The entity is allowed to move to the next trust level. This transition can be represented as
δ (T1j, {E}, L)→(T2j, L)

The evaluation of trustworthiness is based on two relationships between recommendations and context. In the first case it is a reputation based on the initial trust, value and the second one is context dependent [9]. For example, if a passenger who has no previous relationship with any of the entities like authority, the ITV for the context free trust or the general trust (50%) and based upon the context with which the journey is undertaken, will be fixed. In the case of a normal situation, the context aware trust varies according to the degree of importance. For a normal situation the degree of importance is 25 %, for a conference it is 50%, in case of international trading and affairs, it is 75 % and for epidemics or any national alerts the ITV will be taken to be 100%. The degree of importance in assigning ITV is reflected in the weighted factor mentioned in the model.
Let the init ial trust value (ITV) for various contexts are represented as T0e, T0t, T0p,T0a. The trust of an entity with its initial trust valueT0e at Information Exchange Context (IEC) can be predicted as in (1).

$$\text{Trust@IEC}=[\text{T0e}+1-p(s)] \qquad (1)$$

Similarly equations (2), (3), (4) predict the trust values at the Internal Task Context, Internal Process, Context, External Attack Context with initial trust values T0t, T0a, T0p respectively.

$$\text{Trust@ ITC} = [\text{T0t} + 1-p(s)] \qquad (2)$$

$$\text{Trust@ IPC} = [\text{T0p} + 1-p(s)] \qquad (3)$$

$$\text{Trust@ EAC}= [\text{T0a} + 1-p(s)] \qquad (4)$$

6. Conclusion

The distributed provenance technique is modeled and deployed in a spurious and counterfeit drug control system to gauge the trustworthiness of the drugs. The information security assurance model is necessary in order to continue the business in a secure environment. The provenance model provided will keep the availability and security of the information in a balanced state. The ISG, ISC and ISR help in identification of all the possible risk associated with the assets. These techniques help in maintaining the original document from the attackers, in case of any modification by the internal user only the duplicate document is created and reported to the higher authority. In addition to the products, the people who involved in the processes can also be traced for illicit activities. This helps in enhancing the development of product of the organization. It evaluates the total risk involved in a process and also provides the mitigation policies in order to extend and continue the business process. The federated web services, collaborating with mobile query services can solve the problem of anti social activities to some extent. The bio inspiration model is basically secured for data provenance and various assertions are proposed in the mobile tracking model.

References

[1] Shishir Kant Jain.: “The Spurious Drug Menance and Remedy”, Health Administrator, Vol: XIX No.1 pp.29--40

[2] Ragib Hasan.,et.al, “Preventing History Forgery with Secure Provenance”, ACM Transactions on storage,Vol: 5, No.4, Article 12.

[3] Gambetta, D.: “Can we trust trust? in Trust: Making and Breaking Cooperative Relations”, Gambetta, D. (ed.), Chapter 13, (1988). University of Oxford: 213–237.

[4] Trbovich, P.L., Patrick, A.S. (2004): “The impact of context upon trust formation in ambient societies”. Position paper presented at the CHI (2004) Workshop on Considering Trust in Ambient Societies, April 26, Vienna, Austria.

[5] Peter, C. Chapin, Christian Skalka, and Sean Wang.: “Authorization in trust management: Features and foundations”. In: ACM Computing Surveys, Vol 40, Issue 3, Article No.9 August (2008).saz

[6] Sabater, J., Sierra,C. “REGRET: A reputation model for gregarious societies”. In: Proc of the 4th workshop on deception fraud and trust in agent societies, Montreal, Canada, (2001), pp. 61–-70.

[7] Syed Mubashir Ali, Tariq Rahim Soomro, “Integration of Information Security Essential Controls into Information Technology Infrastructure Library – A Proposed Framework”, International Journal of Applied Science and TechnologyVol. 4 No. 1; January 2014,pp. 95.

[8] Chulki Jeong and Sungjin Ahn, “A Study on the Improvements of Information Security Management System for Environment Education Institutes”, International Journal of Security and Its Applications Vol.8, No.4 (2014), pp.247-252 http://dx.doi.org/10.14257/ijsia.2014.8.4.22.

[9] Ms. Deepti Juneja Ms. Kavita Arora Ms. Sonia Duggal, “Developing Security Metrics for information Security measurement system”, International Journal of Enterprise Computing and Business Systems ISSN (Online) : 2230-8849 http://www.ijecbs.com Vol. 1 Issue 2 July 2011.

[10] Igli Tashi, “Solange Ghernaouti-Hélie, Security metrics to improve information security management”, In Proceedings of the 6th Annual Security Conference, April 11-12, 2007, Las Vegas, NV, www.security-conference.org.

[11] Lewis, Riyana, Louvieris, Panos, “Cyber security Information Sharing: A Framework For Information Security Management In Uk Sme Supply Chains”, Twenty Second European Conference on Information Systems, Tel Aviv 2014.