A Predictable Information Security Based Context Aware Trust Model for Organization Management: A Statistical Analysis

Vinod Duraivelu[1*], Chandrasekaran Subramaniam[2]

[1] Department of Computer Science and Engineering, Sathyabama University, Chennai, 600 127, Tamil Nadu, India.

[2] Department of Computer Science and Engineering, Sri Ranganathar institute of engineering and technology, Coimbatore, Tamil Nadu, India.

* Corresponding author.; dvinopaul@gmail.com

Manuscript submitted February 01, 2016; accepted April 8, 2016.
doi: 10.17706/jsw.11.6.577-588

Abstract: The objective of the work is to propose a Predictable Context Aware Trust (PCAT) model for achieving organisation information security in the presence of suspicious entities and authorities. The properties of the PCAT model are studied including the suspicion stack pertaining to the members in different contexts. A reputation score is rewarded based on the contexts in which the information exchange is done. The proposed information trust model encompasses the trust level of the members, degree of suspicion in the information, the levels of privacy, reputation values of the trustees and their trust relationships to predict organization security. An airway passenger guidance system is taken up for statistical analysis. A conceptual and hierarchical trust pyramid is considered at different context levels and the formal implications are derived using context sensitive standard deontic logic. The formal specifications of a passport checking sub system are given in Temporal Logic of Actions (TLA$^+$) which uses certificate authorities and trustees to evaluate passengers by assigning suspicious values.

Key words: Trust value, suspicion stack, context aware, standard deontic logic, reputation.

1. Introduction

In any organization that demands a highly secured information system, the members at various levels as per the hierarchy within or outside the organization are allowed to interact under different contexts based on their trusted and suspicious behaviour .In the context of information exchange where members interact the expected outcome depends on the permissible limits of trust values of the involved entities The information exchange requires a secure and a threat free trust model under various levels of suspicion. 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 [1]. 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 on another varies from one context to another. For a dynamic system, which considers current and future trust levels has to be predicted and managed efficiently. In a situation where a trust value to be established for an entity which is not part of the information exchange, a feedback mechanism is suggested for recommendation. In this model, there are possibilities of deceptive recommendations which increase model's susceptibility to attacks. In the evidential trust model [2], the trust calculation provides reasoning about the future interaction, but the essential security in the presence of attacks is not considered. The earlier Context Aware Trust model which is based on interaction between entities evaluates the direct trust associated with an entity based on the outcome of the interactions [3]. A well defined formulae or some logic of permissible implications was applied to determine the rights associated with each entity to move on to next higher trust level. These rules are specified using standard deontic logic [4] which deals with obligation, permission and related concepts. In case of Trust Management systems the permissibility or authorization is expressed in terms of finding a proof representing successful interaction, with the use of suitable logic [5]. 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. The trust value 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. The context implies how and why the members trust the information given to them [6]. In this paper, a Predictable Context Aware Trust model PCAT proposed. This trust model identifies suspicion values of the trust members in each and every context using a suspicion stack. [7] The model also considered which entities have the right to communicate to whom and when the PCAT model is applied to an airway passenger guidance system where the specifications for the passport checking subsystem are formally specified using Temporal Logic of Actions(TLA) language.

2. Proposed PCAT Trust Model

The proposed trust model predicts a trust value for each and every member involved in direct or indirect interaction by evaluating its suspicion value during that scenario. This suspicion value serves to predict the trust value for a member based on the previous reputation and the current trust value in the particular context. The trust value of a member changes based on the outcome of the interaction, the value may decrease, when the suspicious stack value of the member is high and not based on time The earlier context aware trust model based on the interaction between the members had stated that if there is no future interaction between members the trust value will decrease with time. This contradicts the fact that when a member is assigned a trust value in each context, even if there is no interaction, the trust value of that member will remain unchanged. Thus, it only results in the member being irrelevant or redundant in that particular interaction in that scenario.

2.1. Suspicion Value

The suspicion values for the members in each and every context are maintained in a stack called the Context Suspicion Stack (CSS). The suspicion values in the stack range from low to very high, CSS = {L, M, H, VH} where L represents low suspicion value of the member. Similarly M, H, VH represent medium, high and very high suspicion values of the member respectively. The top of the stack points to the current suspicion value which determines the trust value for an entity, process, task and attack which are represented as {e, p, t, a}.

2.2. 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. Based on the various contexts explained above, the corresponding suspicion level in the respective suspicion stack is checked and then trust value is predicted. If the suspicion value in the stack changes from high to low, then the trust value increases else 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 Fig. 1.

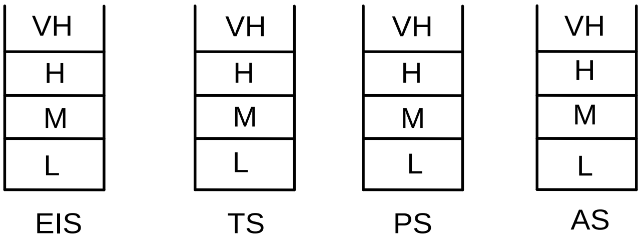

Fig. 1. Various context suspicion stacks.

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. In the lowest level of the trust model, the incoming items may be considered as the symbols in 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.

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 be 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

$$(T_{ij}, C_j, ST) \rightarrow T_{(i+1)j}, \text{ where } j=\{e, t, p, a\};\ i=\{0,1,2\}$$

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

$$\delta\ (T_{1j}, \{\mathrm{E}\}, \mathrm{VH}) \rightarrow (T_{0j}, \varepsilon) \text{ where } j=\{e, t, p, a\}$$

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 T_{0j} 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

$$\delta\ (T_{1j}, \{E\}, H) \rightarrow (T_{0j}, \varepsilon)$$

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

$$\delta\ (T_{1j}, \{E\}, M) \rightarrow (T_{0j}, \varepsilon)$$

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

$$\delta\ (T_{1j}, \{E\}, L) \rightarrow (T_{2j}, L)$$

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 weightage factor mentioned in the model.

Let the initial trust value (ITV) for various contexts are represented as T_{0e}, T_{0t}, T_{0p}, T_{0a}. The trust of an entity with its initial trust valueT_{0e} at Information Exchange Context (IEC) can be predicted as in (1).

$$\text{Trust@ IEC}= [T_{0e} + 1\text{-}\ p(s)] \tag{1}$$

Similarly equations (2), (3), (4) predict the trust values at the Internal Task Context, Internal Process Context, External Attack Context with initial trust values T_{0t}, T_{0a}, T_{0p} respectively.

$$\text{Trust@ ITC} = [T_{0t} + 1\text{-}p(s)] \tag{2}$$

$$\text{Trust@ IPC} = [T_{0p} + 1\text{-}p(s)] \tag{3}$$

$$\text{Trust@ EAC}= [T_{0a} + 1\text{-}p(s)] \tag{4}$$

2.2. Deontic Logic

The trust can be managed in each context using a set of rules or implication to specify if a member can be trusted. These implications that specify the trustworthiness for a member 'a' in a particular context in a system based on the suspicion values in that context can be given using standard deontic logic having the following statuses (i) Permissible (PE), (ii) Impermissible (IM) (iii) Obligatory (OB).

A member 'a' is acceptable if it is defined (df) necessarily (□) to have a low suspicion value (L), then it is obligatory that it has to be assigned trust. This may be represented as:

$$OB_a = df \,\square\, (L \rightarrow a)\ .$$

A member 'a' is defined such that it is possible (◊) for it to have a low suspicion value, then it is permissible that a trust value can be assigned to that member. It may be represented as:

$$PE_a = df\ \lozenge\ (L\ \&\ a)\ .$$

It is impermissible to assign trust for a member 'a' if it necessarily has a suspicion value other than low. This is represented as:

$$IM_a = df \,\square\, (a\rightarrow \sim L)\ .$$

3. Mathematical Model

The prediction of context aware trust values based on ITV of the entity in unknown situation for known and unknown trustees can be done [10]. The context aware trust can be predicted by bringing a mathematical model of the above. Let the trust value of the system in a given context at a given time be represented as $T_t(C_{ij})$ where '*i*' represents the particular context among different contexts considered and 'j' represent the various capacity levels. The different capacity levels in the organization may be represented as 1. Entity Capacity Level 2. Task Capacity level 3. Process Capacity level 4. Attack Capacity level 5. System Capacity level. The role based trust provides role based authority which can be used to express threshold and separation of duty policy [11]. To explain the role and the capacity of various entities in an organization a generic trust pyramid with different trust levels is shown in Fig. 2.

If $T_{(t\text{-}1)}$ represents the previous trust level of the Organization,

C_i represents the given context i and P_j(s) represents the probability of suspicion at capacity level j, then the

system trust at a given context 'i'at in a given level j can be mathematically expressed as

$$T_t(C_{ij}) = T_{(t-1)}+ \prod_{j=1}^{m} (1-P_j(s))C_i] \tag{5}$$

That is, the trust value of the organisation can be predicted by adding the previous trust level of all the entities in all contexts and the overall non suspicion value at different capacity levels where $T_{(t-1)}$ =Previous trust level.

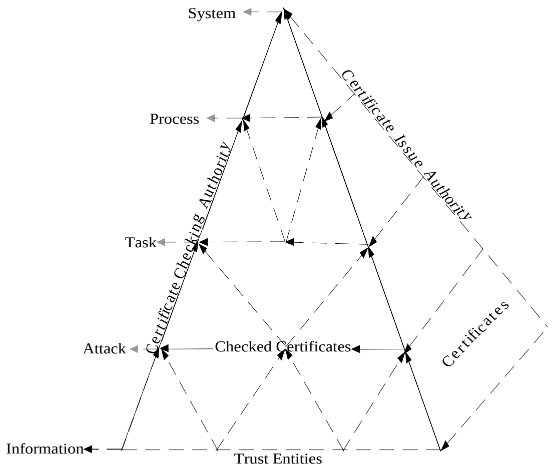

Fig. 2. Trust pyramid.

C_i = weightage assigned to the capacity levels C_i.

P_j (s) =Probability of Suspicion at level j.

The trust evaluation is depending upon both relationship and quality attributes based on reputation[9]. For example, let the previous trust value $T_{(t-1)}$ be 0.4 and the weightage assigned to the capacity levels C_i be 4,3,2,1 and the probability of suspicion values be VH=0.8, H=0.65, M=0.5, L=0.2.Then the current trust value can be calculated using equation (5).

$$T_t(C_{41})=0.45+((1-0.2)\times1)=1.25 .$$

Table 1. Evaluation of Trust

Contexts	Previous Trust Value	Weightage of the Capacity Level	Probability of Suspicion	Context Trust Value
Information Context	0.45	1	L=0.2	1.25
Task Context	0.35	2	M=0.5	1.35
Process Context	0.25	3	H=0.65	1.3
Attack Context	0.15	4	VH=0.8	0.95
			Total	4.85

From Table 1, the organization trust value can be predicted by adding the trust values at each and every context. Thus here it can calculated be as the sum of the entries in the last column, 1.25+1.35+1.3+0.95=4.85. From the above result it is implied that the trust value of a system should be in the set range. If the trust value goes below 4 which is only possible when the weightage of the capacity level decreases, then the system is said to become non-trustworthy.

4. Case Study: A Statistical Approach for Airway Passenger Guidance System

The proposed Predictable Context Aware Trust (PCAT) Model has been applied to Airway Passenger Guidance System where interactions are allowed between the passenger and the various authorities based on the trust certificates and the suspicion levels at each context. The various authorities include Passport check Authority, (PCC) Passport Issue Authority (PIA), Ticket Check Authority (TCA), Ticket Issue Authority (TIA), Custom Check Authority (CCA), Immigration Authority (IMA) and the Chief Airport Authority (CAA). The various trust certificates include the Passport Checked Certificate (PCC), Ticket Checked Certificate (TCC) and Immigration Checked Certificate (ICC). At each context, the various trust certificates are checked and only if there is no suspicion (i.e.) if the certificate is valid, the passenger can move on to the next level in the system. Standard deontic logic is used to specify the appropriate conditions to assign a trust value to a passenger to move on to next level in the system. This is given using a trust pyramid which specifies the various trust levels and certificates. Here the standards of information security have been followed and extended in controlling organization framework. A key factor for achieving optimal security levels within security chains is the management and sharing of cyber security information with specific metrics [11].Similarly in the previous work, the approach considered was organizations frame work. The aim of information security is to ensure business continuity and minimise business damage by preventing and minimizing the impact of security incidents [10].Information trust values have taken are in a air passenger guidance system in order to ensure that the specific passenger to travel as a trusted person, the previous work which specifies the information security approach to overcome the possible attack in a trusted organization. The enhancement suggested is shown in Fig. 3 using various approach to calculate security based information flow for a trusted organization .

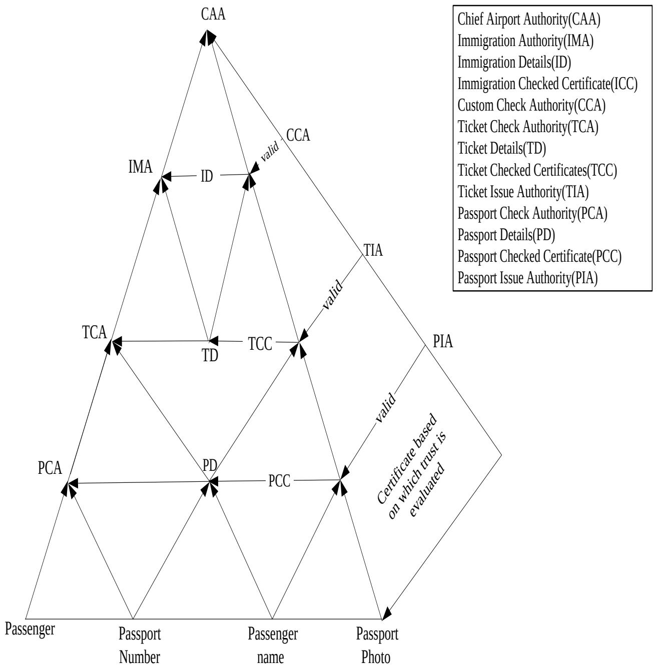
CAA
IMA
ID
valid
CCA
TIA
TCA
TD
TCC
valid
PIA
valid
PCA
PD
PCC
Certificate based on which trust is evaluated
Passenger
Passport Number
Passenger name
Passport Photo
Chief Airport Authority(CAA)
Immigration Authority(IMA)
Immigration Details(ID)
Immigration Checked Certificate(ICC)
Custom Check Authority(CCA)
Ticket Check Authority(TCA)
Ticket Details(TD)
Ticket Checked Certificates(TCC)
Ticket Issue Authority(TIA)
Passport Check Authority(PCA)
Passport Details(PD)
Passport Checked Certificate(PCC)
Passport Issue Authority(PIA)

Fig. 3. Airway passenger trust levels and certificates.

At the first level in the trust pyramid, the passenger submits the various passenger details to the Passport

Checking Authority for verification. The PCA has to ensure that the certificate issued by the PIA is valid. The PIA is checked and issues PCC which along with the passport details passes on to the TCA. The TCA verifies the ticket details (TD) and then issues the TCC. Similarly the trust certificates are checked in the other higher levels based on the suspicion values and the trustworthiness of an entity. In this manner, the trust for the entire organization can be established and managed. Consider the interactions in the Information Exchange Context where the passport details of the passenger are checked. As each detail is verified, the top value of the context suspicion stack should be checked for a low value to ensure a trusted interaction between the members involved. In the illustrated scenario, the passenger is guided by an airway guidance system at the airport. Initially the passenger encounters the passport verification authority and submits the needed details. The passengers submit each of the passport details like the passport number, the expiry date of the passport, the code number of the passenger, the passenger's name to the checking authority. When the passenger details are checked, the contents of the suspicion stack are also checked to see if the stack top points to Low. A low suspicion value indicates that the system is at a trusted level and can proceed to get the next details at the next trust level. The passenger details are sent through the channel which may be subjected to external attack. The proposed trust model resolves this by checking if the top of the External Attack Context suspicion stack is Low, only then the member can move to the next interaction. Fine grained access [12] control is possible by using a formal specification policy that can be understood by both managers and interconnected systems that must make decisions to permit or deny access. In order to give clear picture policies of various authorities at various capacity levels has been formally specified in TLA+.

The formal specifications for the Information Exchange context have been given using TLA+ as given below.

```
---------- MODULE Passport Check -----------------
   EXTENDS Naturals
   VARIABLE Pno, Dob, Codeno, Data, PD
   STRING Pname, IssueAuthority
   VARIABLE PassportData, Channel, StackTop
   TypeInvariantDetails == PassportData \in
   {Val: Pno, Dob, Codeno,
   String: Pname, IssueAuthority,
   ack: {0, 1}, rdy: {0, 1}}
   TypeInvariantChannel == Channel \in
   {Val: Data,
   ackb: {0, 1}, rdyb {0, 1}}
   TypeInvariantSusStack==Stack \in
   {Val: PD, st: {L, H, VH, M}
   TypeIn == /\TypeInvariantDetails
   /\ TypeInvariantChannel
   /\TypeInvariantSusStack
   --------------------------------------------------
   InitPassport == /\ TypeIn
   /\ PassportData.ack=PassportData.rdy
   CheckPno (a) == /\ PassportData[a].ack=1
   CheckDate (b) == /\ PassportData[b].ack=1
   CheckCode (c) == /\ PassportData[c].ack=1
   CheckSTop (d) == /\ StackTop[d].st=L
   (*Checking if Passport is valid or not*)
```

```
PassportValid ==   /\ CheckPno (a)
/\ CheckDate (b)
/\ CheckCode (c)
TrustedTransaction==/\CheckSTop (d)
(*Passport is termed invalid even if one of the checking conditions is not satisfied*)
PassportInvalid == \/ ~CheckPno (a)
\/ ~CheckDate (b)
\/ ~CheckCode (c)
\/~CheckSTop (d)
Send (i) == /\ Channel.ackb = Channel.rdyb
/\Channel'= [Channel
EXCEPT!.Val=a, !.rdyb=1-@]
(****************************************)
(*Sends each attribute of the passport to the buffer where it is checked*)
Rcv (i) == /\ Channel.ackb # Channel.rdyb
/\ Channel' = [Channel EXCEPT
!.ackb=1-@]
(***************************************)
(* The attributes of the passport are received *)
Nextdetails == /\ [(\E a \in Pno), (\E b \in Dob),
(\E c \in Codeno)] : Send (a)
\/ Rcv
/\PassportValid
/\TrustedTransaction
\/PassportInvalid
(*Conditions to be satisfied to move to next Passenger*)
SpecPassport == InitPassport
/\ [] [Nextdetails] PassportDetails, Channel
--------------------------------------------------
THEOREM SpecPassport => [] [TypeIn]
= = = = = = = = = = = = = = = = = = = = = = = = = = = =
```

4.1. Trust Implication

The interactions for verifying the passenger details at the various levels in the trust pyramid are given by the following trust implications.

4.2. Passport Check

The passenger (PAS) goes to the Passport Check Authority (PCA) based on the trust over the PCA and this is denoted by:

PAS →PCA

Now, the PCA verifies the Passport Details (PD) like Passport Number (pno), Passenger name (pname), photo, Date of Birth (dob), validity (val) and then forwards it to Passport Issue Authority (PIA).

PCA→PCA pno/PCA dob/PCA pname/PCA photo/
PCA val/PIA

PCA sends the PD through the channel based on the trust on channel. Then the PIA certifies the PD provided by PCA and returns valid, invalid, expired, or fake.

PIA→ valid /invalid/ expired /fake

Only if the certification is valid the PAS can be given a Passport Checked Certificate (PCC) and is allowed to carry on to next trust level. The standard deontic logic implications for permissible and impermissible conditions for assigning trust to a passenger are based on the validity of passport details and PCC. This can be represented as:

PEPAS ↔OBPCC

IMPAS↔OB~PCC

The passenger is permissible to move to next trust level only if he obligatorily possess a PCC.The variable set V contains the variables like Passport Checking Authority, Passenger and Passport Issue Authority. The terminal set T contains the terminals which include the passport number, passenger name, and date of birth, photo, and validity details of passport.

V={PCA,PAS,PIA}

T={pno,pname, dob, photo, val, pvalid, pinvalid, expired, fake}

4.3. Ticket Check

After the passenger has given the Passport Checked Certificate (PCC), the advances to the next trust level at Ticket Checking Authority (TCA).

This implication is represented as

PAS (PCC) →TCA

The TCA will verify all the Ticket Details like Ticket Number (tno), destination (dest), source, class of journey (class), date of journey (doj) and sends the passenger to the next level in the trust tree. These implications are represented as

TCA→TCA tno/TCA dest/TCA source/TCA class/

TCA doj/TIA

The TLA then verifies the ticket and issues the Ticket Checked Certificate (TCC). Only when the TCC is valid, the passenger is trusted to go to the next level of checking. This implication is represented as

TIA→tvalid/tinvalid for ticket valid and invalid

V= {TCA, PAS, TIA}

T= {tno,dest,source,class,doj,tvalid,tinvalid}

Now the trust between the entities is managed with the help of standard deontic logic. The passenger is permissible to move to the immigration check only if he possesses the TCC, which can be represented as:

PEPAS ↔OBTCC

IMPAS↔OB~TCC.

4.4. Immigration Check

In the next level of trust, the passenger passes through the Immigration Check Authority (ICA) checks the various details like the health certificate (hc), the validity of visa (val), purpose of visit (pof). These implications are represented as

PAS (TCC) →ICA

ICA→ICA hc / ICA val / ICA pof /CCA

The Customs Check Authority (CCA) certifies that the details passed by ICA are valid and ensuring trust, the passenger is allowed to the next trust level.

CCA→acc/rej

V= {ICA, PAS, CCA}

T= {hc, val, pof, acc, rej}

The representation in standard deontic logic to specify that it is permissible to assign trust to a passenger when he possesses valid ICC is given as

$PE_{PAS} \leftrightarrow OB_{ICC}$

$IM_{PAS} \leftrightarrow OB_{\sim ICC}$

Table 2. Association of Members in Airway Passenger Guidance System

Context	Entities	Trustees
Internal Process	Immigration Details	PAS, IMA, CCA
Inner Task	Ticket Details	TCA, PAS, TIA, TCC
External Attack	Channels through which PD are sent for verification	PCA
Information Exchange	Passport Details Name	PAS, PIA

The various entities and trustees at various contexts in an airway passenger guidance system is tabulated in Table II.

Table III illustrates the trust value predicted in External Attack Context. The Initial Trust Values (ITV) are considered to be 0, 0.2, 0.4, 0.6, 0.8, for each of these values and the suspicion values as L=0.2, M=0.5, H=0.65, VH=0.8, the Predicted Trust Value (PTV) is calculated using equation (8).

Table 3. Trust Value predicted in External Attack Context

	Suspicion Values				
ITV	0.2(L)	0.5(M)	0.65(H)	0.8(VH)	PTV
0	3.2	2	1.4	0.8	7.4
0.2	3.4	2.2	1.6	1	8.2
0.4	3.6	2.4	1.8	1.2	9
0.6	3.8	2.6	2	1.4	9.8
0.8	4	2.8	2.2	1.6	10.6

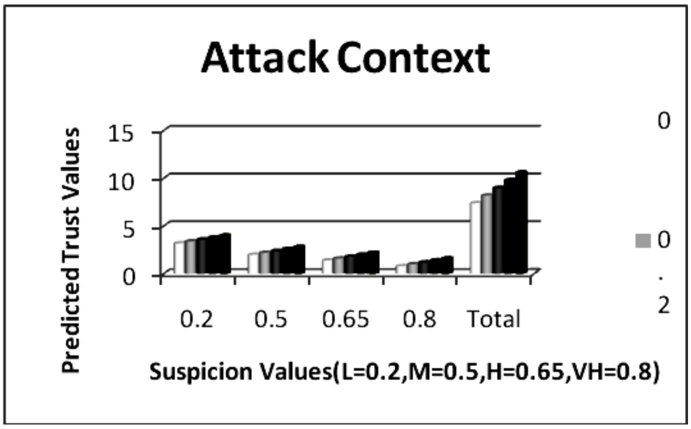

Fig. 4. Suspicion values Vs predicted trust values for external attack context.

In Fig. 4 let the different shades indicate the Initial Trust Values. For the suspicion values along the x-axis, the predicted trust values is said to decrease as the suspicion value increases from Low to Very High. At each ITV the trust values are added to get the overall trust of the organisation. As the Initial Trust Value keeps increasing the Trust value of the organisation is also seen to increase. By setting the appropriate range for the ITV, the organisation trust can be predicted at the given Attack Context.

Similarly Table 4 and Fig. 5 illustrates the predictability of the organisation's trust value at the Information Exchange Context.

Table 4. Trust Value Predicted in Information Exchange Context

	Suspicion Values				
ITV	0.2(L)	0.5(M)	0.65(H)	0.8(VH)	PTV
0	0.8	0.5	0.35	0.2	1.85
0.2	1.0	0.7	0.55	0.4	2.65
0.4	1.2	0.9	0.75	0.6	3.45
0.6	1.4	1.1	0.95	0.8	4.25
0.8	1.6	1.3	1.15	1	5.05

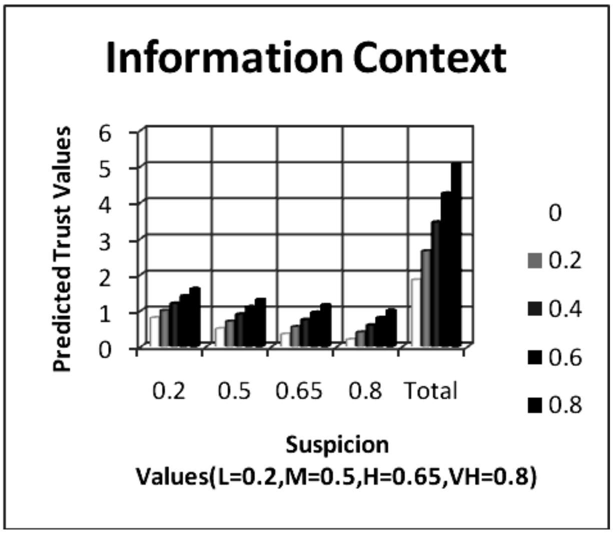

Fig. 5. Suspicion values vs predicted trust values for information context.

5. Conclusion

In the proposed model, the trust value of an organization is predicted based on the contexts in which its internal and external actors with their various capacity levels are interacting .The trust level and the trust entities in various levels are represented as a trust pyramid. The concept of a suspicion stack is introduced whose elements are the values of suspicion due to misbehaviour within the organization and the trust is managed using the standard deontic logic. The context aware trust is determined by considering the previous trust value and the weightage of the capacity level of the member or entity. Through the formal specifications of an airway passenger guidance system, a scenario is considered in which a passenger is allowed to proceed to the next level of checking only after being certified by the authorities with respect to the trusted certificates. The various levels like passport check, ticket check and immigration check in the airport organization are considered to validate the model. The logic and the reputation based trust can also be determined in the contexts of internal process and external attack using the PCAT model. The effectiveness of the model lies in the fact that the suspicion stack is trusted to predict the trust values for the members and entities in an organization .The accuracy of the prediction improves as the height of the pyramid or in other words the number of capacity levels increases. When a new member or entity is introduced in to the organization or if the organization policy is revised, the new trust logic has to be applied.

References

[1] Gambetta, D. (1988). *Can We Trust in trust: Making and Breaking Cooperative Relations*. University of Oxford: 213–237.

[2] Sabater, J., & Sierra, C. (2001), Regret: A reputation model for gregarious societies*. Proceedings of the 4th Workshop on Deception Fraud and Trust in Agent Societies* (pp. 61-70), Montreal, Canada,

[3] Mohammad, G. U., Mohammad, Z., & Sheikh, I. A. (2008). CAT: A context aware trust model for open and dynamic systems*. Proceedings of the 2008 ACM symposium on Applied computing*.

[4] McNamara, P. (2009). Standard deontic logic. *The Stanford Encyclopedia of Philosophy*

[5] Peter, C. C., Christian, S., & Sean, W. (2008): Authorization in trust management: Features and foundations. *ACM Computing Surveys*, *40(3)*.

[6] 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*.

[7] Shi, J. Q., *et al.* A trust model with statistical foundation.

[8] Florina, A., *et al*. (2003): PTM: A pervasive trust management model for dynamic open environments. *UBISEC*.

[9] Santtu, T., *et al*. (2006): Context aware trust evaluation functions for dynamic reconfigurable systems.*WWW May*. Edinburgh, UK.

[10] Mozhgan, T. (2009). Situation aware trust management. *RecSys'09 October*.

[11] IEEE symposium on security and privacy. (2002). *IEEE Computer Society Trust*, 114-130.

[12] Dynamic trust management. *IEEE Computer Society*, 44-52.

Vinod Duraivelu was born in Chennai, Tamil Nadu, India in 1983. He completed his under graduate degree in bachelor of technology in information technology with First Class at Anna University, Chennai, Tamil Nadu, India in 2005. And he completed his post graduate degree in master of technology in computer science and engineering with First class with Distinction at Anna University, Chennai, Tamil Nadu, India in 2009. Now, He pursuing his doctor of philosophy in information security at Sathyabama University, Chennai, Tamil Nadu, India. He resently working as an associate professor and the head of the Department of Information Technology at Sri Ramanujar Engineering College, Chennai, Tamil Nadu, India since 2005. He have published articles in Springer in Japan, 2010, IEEE in Singapore, 2012, ACM in 2013, Scientific Journal in 2014, Currently focusing on information security architecture and information flow control.

Chandrasekaran Subramaniam was born in Uttukuli, Erode district, Tamil Nadu, India in 1957. He have completed his under graduate degree in bachelor of engineering in electronics and communication engineering with First Class at Coimbatore Institute of Technology, Tamil Nadu, India in 1980; He have completed his post graduate degree in master of engineering in computer science and engineering at Regional Engineering College, Tiruchirappalli, Tamil Nadu, India in 1993 and He have completed his doctor of philosophy in information and communication engineering at Anna University, Chennai, Tamil Nadu, India. He presently working as a professor and the dean at the Department of Computer Science and Information Technology at Sri Ranganathan Institute of Engineering and Technology, Coimbatore, Tamil Nadu, India since 2014. He have published articles in IASTED (Austria, 2001) IPSOC (France, 2005), HPCNCS (USA, 2007), He currently focusing on software reliability and security architecture.