IJCTA, 9(36), 2016, pp. 561-572

An Efficient Technique for Customer Analysis and Categorization over Fault Tolerance in Online Transaction Processing System

L. Javid Ali* and G.S. Anandhamala**

Abstract : E-commerce has ushered in a reality where customers increasingly purchase products and services through online solutions offered by banks, merchants and various other players. "Conversion", "barriers to conversion" etc. have become the mantra in digital organization's never-ending quest to simplify the check out process. There are numerous studies that seek to simplify various facets of check out process – "sign-in process", "streamlining number & order of check out steps" etc. mostly focusing on the happy path scenario. That being said, customers also endure many "error scenarios" during check out process, be it user authentication, payment card verification, address validation etc. While "Error recovery" is usually employed to mitigate such scenarios, we notice that this is not universally applied to all error scenarios during checkout. In this paper, we focus on a way to improve customer's experience as they authenticate their payment card credentials using "fault tolerance" scheme. Banks require customers to key in "one-time password (OTP)" to prevent frauds in credit card transactions. OTP is usually sent to customer's mobile devices (for the most part) and in some cases customer's email address. As customers are required to key in the OTP, they often make mistakes ranging from simple "typos" to down-right typing in incorrect numbers such as the "request ID". Currently, at least in Indian e-commerce scenario, sessions are immediately terminated leading to poor user experience and lost sales for merchant. Based on customer's past record with a particular merchant / bank, number of legitimate and successful transactions, membership status (if applicable), we propose that system assign a "fault tolerance" limit to each customer, which would allow eligible customers additional attempt(s) to key in new OTP after they successfully answer challenge questions. Thus "fault tolerance" scheme would allow customers to "recover from error" and complete the transaction, invariably improving their experience and merchant's bottom-line.

Keywords: Fault Tolerance, Risk Analysis, Web Applications, Online Transaction Processing.

1. INTRODUCTION

Literature defines Fault tolerance as a property that enables a system to continue operating properly in the event of the failure of (or one or more faults within) some of its components. As the name implies, a fault-tolerant design allows equipment to continue functioning in the presence of hardware faults. In a similar note, an error-tolerant design is one that does not unduly penalize user or human errors. It is the human equivalent of a fault-tolerant design. Use of constraints that prevent occurrence of error in the first place is ideal approach. However, it is not always possible to prevent errors especially in scenarios requiring user interaction. The next best approach is to try to limit the impact of the error. A good example in case of user interface design is the dialog box, "Are you sure you want to continue" especially in cases where an error could have considerable impact. On a side note, adding too great a mitigating factor could also

* Research scholar, Sathyabama University, Department of Computer Science and Engineering, St.Joseph's College of Engineering, OMR, Chennai, Tamilnadu, India

** Professor, Department of Computer science and Engineering, Eswari Engineering College, Ramapuram, Chennai, Tamilnadu, India

end up becoming a hindrance and prevent users from completing their task. Limiting the impact of error alone is never sufficient. Users must be afforded an opportunity to recover from the error in a simple and intuitive way and continue with their task where feasible. This is an important facet of error-tolerant design. Algorithm-Based Fault Tolerance (ABFT) is a method for detecting and comparing the computer-induced errors. The parity generation function sets the priority values in order to process the data. This algorithm is not suitable for detecting adjacent large errors in the same block with high insertion rate [1]. Fault detection and fault location techniques are applied over transmission online systems. These types of data transmission are stable and not suitable for dynamic environment. The Quality of Service (QoS) is achieved by minimizing the transmission delay and packet loss [2]. A normal feedback control system is shared with other nodes which reside outside the region. The Networked Control Systems (NCSs) [20] needs the security control in the real world and life applications [3]. An inherently stabilizing system doesn't affect the process variables during the algorithm execution. This system is not suitable for applying node disjoint path algorithm on regular topologies [4]. A stack of randomized intrusion-tolerant protocols are very suitable for Local-Area-Network (LAN) and Wide-Area-Network (WAN) environments with fault tolerance. These protocols are difficult to eliminate the byzantine faults because it targets only performance evaluation on computer network in different perspectives [5]. An adaptive fault-tolerant QoS control algorithm is used to satisfy the application of the sensor system with the help of source and path redundancy level [6]. This algorithm is not reliable for hop-to-hop delivery which is handled by ACK-based data delivery schemes with high reliability. A novel 2-round group key agreement protocol has been implemented over various node failures which fall within the threshold level. This algorithm is more secure than the assumption of Decisional Square Diffie-Hellman algorithm [7]. A distributed data access control scheme is used to eliminate the data security attack, illegal access of the fine grained data access with its control and it minimizes the direct adoption of cryptographic primitives [8]. SCIT (Self-Cleansing Intrusion Tolerance) [10] is not suitable for detection-based Intrusion-Tolerant Servers (ITS) and also not for their components like proxies, ballot monitors, and acceptance monitors. ITS architectures needs better control over the trust and fault tolerance [9]. The RAPID combines the probabilistic flooding, counter-based broadcast, and lazy gossip techniques for achieving the reliability, latency and message overhead occur in these protocols. This protocol is not suitable for sending the REQUEST messages continuously over wireless sensor network because of the performance degradation attacks [11]. Precision Time Protocol (PTP) is used to avoid the collision which occurs between the packets. The synchronization between the slaves prevents the traffic problem. The highest tolerance level has been assigned to the master to protect from failure and to control the slaves continuously [12]. Antagonistic interference is a challenging problem in reliable communication over sensor network from malicious attacks and benign faults. The model analysis focuses on the feasibility and QoS metrics like communication complexity, delay, and efficiency in energy [13]. The algorithm focuses on the network partitioning by overlapping the area with the help of local estimators. The purpose of this work is to minimize the difference and consolidation of various local estimators. The tolerance level is converted from convergence of state estimation [14]. The insider attack gives severe loss to the parameters related to the data availability, latency, and throughput. Several protocols are identified in order to achieve maximum security such as packet drop and packet injection, bad mouthing (ballot stuffing) on the trust management, random attack on the trust management and bad mouthing on the detection scheme [15]. Secure Multiparty Computation (SMC) is a security technique which is used to solve many real world problems in online transactions and various security algorithms. This problem is overcome by using the TrustedPals which is a smart card-based security framework with more efficiency [16]. The existing algorithms have been applied to implement the fault tolerance mechanism which will not support fully in the area of web based online transaction system. The main objective of the proposed work is to achieve the maximum fault tolerance in various levels of security over online transaction. The tolerance level is found based on the threshold value fixed in multiple levels without compromising the available security level. This algorithm acquires input from the user with various thresholds which decides the overall tolerance level of the user and

also maximizes the efficiency in all levels of web application. The rest of the paper provides an overall processing technique of the proposed work.

2. APPROACH

2.1. Understanding & Classifying Customers

A quick background on internet shopping (e-commerce) and customer motivations would help set the context. According to the theory of customer perceived value proposed by Zeithmal [19, 20], he insisted that the customer value is the customer perceived value. Through the model of Internet shopping transactions and the value of stakeholder analysis, a case can be made that five dimensions of the values on e-commerce customer are network platform value, retailer value, logistics company value, third-party payment value and bank value.

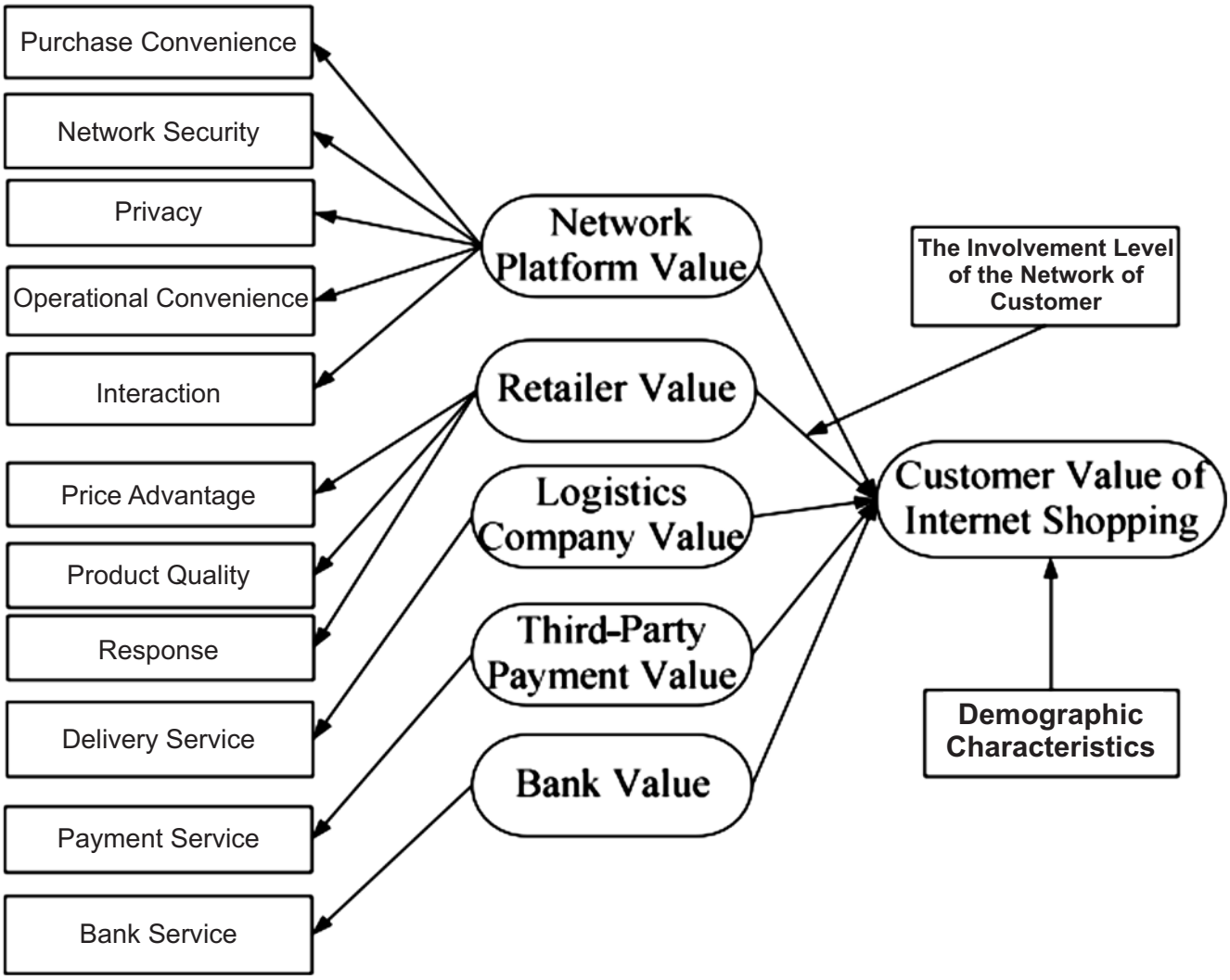

Figure 1: Customer Value Model of E-commerce

In this paper, we focus on third-party payment value and bank value portion on the overall customer value model. Take the case of e-commerce industry that suffers from significant abandonment rates. A 2015 aggregation of statistics from 32 recent studies on e-commerce shopping cart abandonment rates averages to about 70% [17]. Literature defines abandonment rate as the ratio of the number of abandoned shopping carts to the number of initiated transactions or to the number of completed transactions. It is our premise that applying error-tolerant design to this particular use case would positively impact the abandonment rate. That being said, this often means qualifying error recovery mechanism with adequate safeguard and constraints, so security measures are not compromised. In popular literature, Risk tolerance is generally

something tied to an individual customer's investment risk taking capability. In this paper, however, we specifically focus on risk tolerance applied by organization to individual customers based on their past transactional history (successful and abandoned transaction volume and/or transaction amount) with the organization, with processing bank, customer's membership status etc. Based on the aforementioned factors and with appropriate weightage, we propose that customers be classified into different risk profile categories, say "key customers or low-risk customers", "under-potential" and "non-users or high-risk customers". A methodology already in vogue to classify customers in the marketing world is called as RFM model – Recency, Frequency and Monetary Value. Recency refers to duration since last customer purchase. Whereas frequency refers to number of purchases in last year and monetary value refers to their highest spend in that time period. Each attribute can be further broken into sub-categories; purchase within last 90 days, 90 – 180 days with each range weighted appropriately. By assigning values customers may be objectively categorized. There are number of variations of this model in the market too. Case in point is customer categorization and credibility building mechanism in use in Third Party Payment model, especially when it comes to C2C (customer to customer transaction) where buyers and sellers may not necessarily trust each other [18]. Buyers worry if they pay their bill first, their commodities may not be delivered. While the sellers worry if they ship the commodities first, they may not be paid. As and when a transaction is successfully carried out [buyers pay for the product / service, and seller provides service or ships product], TPP system will add credit points to buyers and sellers. The more credit points sellers and buyers gain (see figure 2), the more credibility / trading reputation they gain. This methodology is widely used by marketplace such as Amazon, Ebay etc. as well.

Transaction Amount (Us Dollar)	***Credit Points***
0 – 1	0.1
1.01 – 10	0.2
10.01 – 100	0.5
100.01 – 1000	1
> 1000	2

Figure 2 : Credit Points and Transaction Amount [18]

This is somewhat similar to credit scoring widely employed in the banking industry to determine customer's willingness to pay back loans in a timely manner. A more sophisticated statistical analysis of customer's transaction history could be used to accurately assess the trustworthiness of customer.

2.2. Checkout Process

A thorough study of the possible type / categories of error that end-users make is beyond the scope of this paper. Instead of we focus on the typical errors made during check-out process and how it correlates to the cart abandonment percentage referenced in the sections above.

1. Having unnecessary form fields like non-payment related question such as "how did you find us?".
2. Too many manual steps. Forcing user to select / enter city, state and country where auto-filling based on postal / zip code would reduce the number of clicks for end user. Or forcing to type billing and shipping address twice even if they are the same.
3. Forcing people to create an account with distractions such as "email verification" and other additional fields. These steps encourage user to drop off the "shopping funnel".
4. Emphasizing coupon codes, which is another distraction for users who tend to use search engine to find coupons instead of completing the transaction.
5. Offering limited payment options.
6. Stringent payment process that offers no scope for error recovery. Some examples are listed below:

- Error message placement on top of the form which users miss and are timed out
- Reliance on server-side validation and not leveraging client side validation. For example, missing "@" symbol in email field could be validated without sending data to server.
- Resetting field data due to simple errors forcing user to type everything back.
- Credit card validation & OTP related errors redirecting users to start from the beginning of the checkout process

2.3. Validation Errors

While many error scenarios referred above may be mitigated through A/B testing and appropriate design remediation measures and indeed are solved for, credit card validation & OTP related errors is often left untouched citing security concerns. It is the considered view of this author that error-tolerant design and security measure is not necessarily a "zero-sum game". Instead, more could be done to improve the error recovery rate without compromising security through usage of risk tolerance and RFM model of customer classification. Not to mention the revenue loss to business due to unrealized transactions that could very well be simple mistakes.

Let us consider few scenarios / customer work flow in the context of an *e*-commerce purchase funnel and how customers are not stopped in their tracks from completing their journey. It starts with product awareness, active consideration and then purchase. Sometime Advocacy is included as a final step.

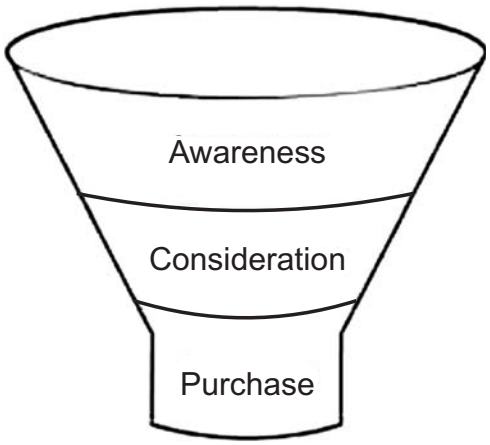

Figure 3: Ecommerce Purchase Funnel

Scenario 1: User A is in his late-40s. He is a loyal and a long-time customer of a well-known consumer goods retailer. He typically purchases product in a physical store but always uses the retailer's loyalty / membership program. Having been introduced to recently launched *e*-commerce solution, he tries to purchase a product online. Having made up to card validation page, he mixes up the OTP with request ID, errors out and is sent back to the beginning of payment process without any recourse.

$$\text{Payment Validation} = \{\text{Success, Product Flow Error, Otherwise}\}$$

$$\text{Product Flow} = \{\text{Product Selection} \cup \text{Product payment}\}$$

$$\text{Product Selection} = \left\{\sum \text{Product} \in \text{Product List}\right\}$$

$$\text{Product Payment} = \left\{\sum (\text{Card Payment} \cap \text{Netbanking}\right\}$$

Scenario 2 : User B is a young tech-savvy professional. She relies on a trustworthy big-name *e*-tailer to purchase all personal care products she requires. Ever conscious of privacy issues, she always tries to avoid creating accounts where feasible and does not like waiting on web pages to load. Unfortunately, she is confronting a situation where OTP generated by bank is being delivered to her mobile device very slowly due to network issues causing her to time-out. She has no other alternative but to start from first step.

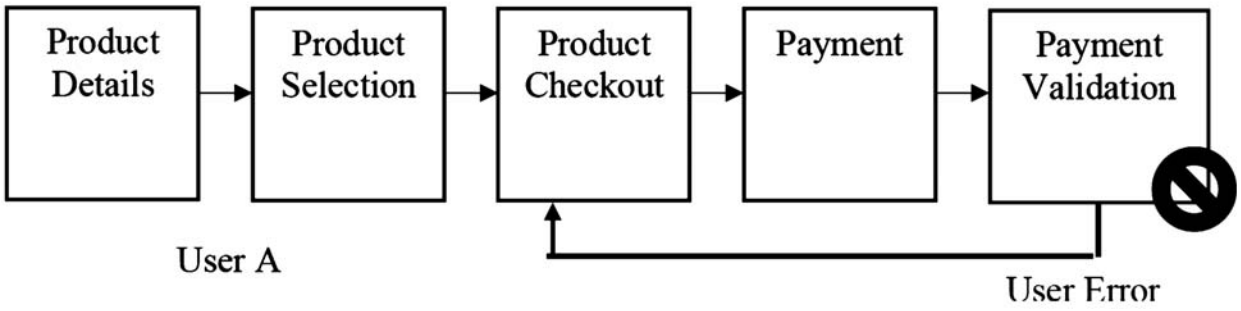

Figure 4: Customer Journey: User A

$$\text{Payment Validation Error} = \begin{cases} 1, & \text{Session} \\ 0, & \text{Otherwise} \end{cases}$$

$$\text{Session} = \begin{cases} 1, & \text{Session Alive} \\ 0, & \text{Otherwise} \end{cases}$$

$$\text{Session Alive} = \begin{cases} \text{True}, & \text{OTP Generation} \\ \text{False}, & \text{Otherwise} \end{cases}$$

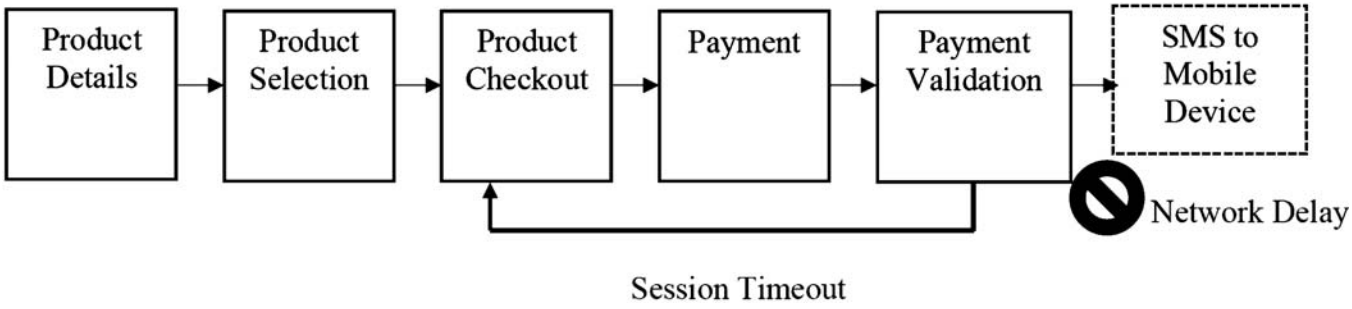

Figure 5: Customer Journey: User B

Scenario 3: User C is a NRI who is in India on vacation. He had been a heavy user of a particular *e*-commerce site but it has been couple of years since he has last used it. He is in the check-out page but is having trouble authenticating as he no longer owns the mobile phone that he initially registered with. OTP is being sent to his old mobile phone now owned by someone else. It seems his only option is to abandon the transaction, update his profile and then return back and he is not thrilled about it.

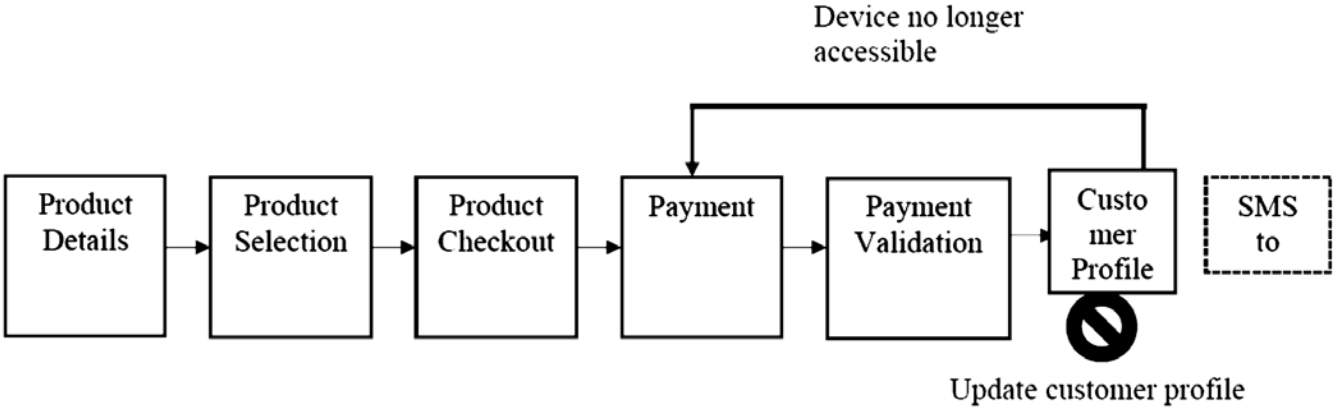

Figure 6: Customer Journey: User C

$$\text{Customer Profile} = \begin{cases} 1, & \text{Status} \\ 0, & \text{Otherwise} \end{cases}$$

$$\text{Status} = \begin{Bmatrix} \text{Satisfied}, & \text{Customer Profile} \\ \text{Update}, & \text{Otherwise} \end{Bmatrix}$$

$$\text{Update} = \begin{Bmatrix} \text{Ok}, & \text{Successful Updataion} \\ \text{Error}, & \text{Device No Longer Accessible} \end{Bmatrix}$$

While the circumstances and customer profile may vary across these 3 scenarios, there is one underlying theme and that is frustrated customers. The source of their frustration is that they are being forced to abandon the purchase, albeit for various reasons; user error, network delays and circumstances, but nevertheless requiring them to start over.

2.4. How does risk tolerance and RFM model work?

But what if we could apply "risk tolerance" scheme and allow customers a path to recover from the error? In the example above, we know that customers would have different recency score – one a first time user but has a strong offline transaction record that is also recent, another a frequent and recent online user and the last one who hasn't interacted for a while in the recent past, a different frequency score and membership status or lack thereof. Next step is to apply weightage to each factor depending on the error cause / circumstance – in case of User 1 it is user error as he is entering request ID instead of OTP. On the other hand, User 2 is getting timed out even as she enters valid OTP whereas User 3 is not interacting as he is not getting the OTP. The type of error could either increase or decrease the weightage to a particular factor (recency, frequency, membership status), which would in turn determine their tolerance score. If the computed score is within the threshold of risk tolerance, then customer may be afforded an opportunity to recover from error by either allowing to answer challenge questions and/or attempting with next OTP without terminating the session. However, if the computed score is more than the risk tolerance of a customer, then the session may be terminated for security reasons.

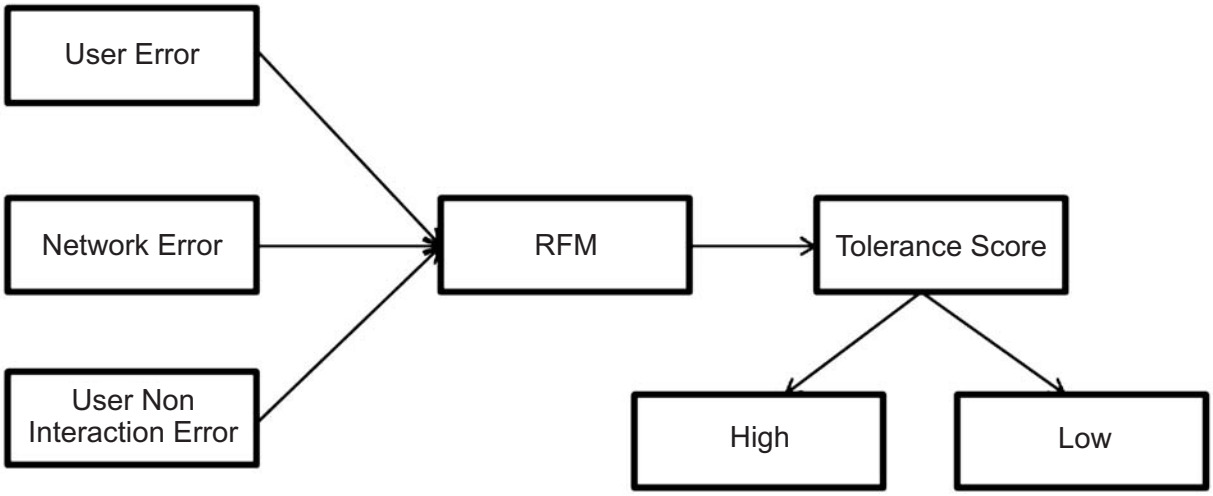

Figure 7: RFM based Tolerance score

3. ALGORITHM

Algorithm credit_calculation()
begin
if(risk tolerance is available) then
begin
check the attribute of risk tolerance as RSattrib;
for each RSattrib do
catergorize the customer as CUScat;

CUScat = {key customer / low risk customer, under potential customer, non-user / high risk customer}
for each CUScat do
begin
check the RFM attribute as RFMattrib;
catergorize the purchase duration from the RFMattrib;
end
end
identify the risk for buyers and sellers;
if (buyer is authentic) then
buyer risk is less
else
seller risk is less
end
credit point is calculated based on the authenticity during transaction;
allocate the credit point to the customers;
end
return credit_points;
end

4. RESULT AND ANALYSIS

Out of three error categories, namely user entry/selection error, network error and user non-interaction error, analysis of user entry/selection error category is shown in the analysis. The analysis is made over a sequence of three levels namely level 1, 2, and 3 that are considered to be user login page, selection page(s) and finally third party payment page. The equations 1 and 2 shows the initialization and user access level related to the proposed fault tolerance technique.

$$Q = \{H(t), \mho\} \tag{1}$$

$$\text{User Access Level} = \begin{Bmatrix} \text{Key Customer, } H(t) & < \mho \\ \text{Under Potential Customer} & \leq \mho \\ \text{High Risk Customer} & > \mho \end{Bmatrix} \tag{2}$$

Where $H(t)$ and $\mho$ is hit count and hit threshold respectively.

4.1. Tolerance Level Fixation

4.1.1. Level$_1$

The tolerance level is fixed based on the propositional count and maximum number of hits in the level$_1$. The faults are categorized in various levels with user access level and number of hits. The Q_1 maintains the user with highest tolerance level at level$_1$. The value of the tolerance level falls between 0 and 1. The equation 3 describes the tolerance level$_1$ calculation.

$$\text{Tolerance level} = \text{Count}(t) * \frac{1}{\text{Max}(H(t))} \tag{3}$$

Where count (t), is the number of hit count.

4.1.2. Level$_2$

The Q_2 maintains the users who are having the highest tolerance level at the level$_1$ and also the number of selections through various input options in the web page. The level$_2$ hit count is based on the zero selection

hit and non-zero selection hit count. In the zero hit count category, the user may select the common options in the web pages whereas in non-zero selection the user selects the options using the available input field and hyperlink. The non-zero selection has two hit count namely fault count $f(t)$ and correct count $I(t)$. If the user level is non-user / high risk category and $f(t) < \omega 1$, then the tolerance level is set as minimum. If the user level is under potential and $c(t) \leq \omega 2$, then the tolerance level is set close to minimum and the maximum threshold is set for the key customer users. The user movement to the next web page is based on the threshold and access level at the Q_1 and Q_2 *i.e.* $level_1$ and $level_2$. The equations 4, 5, 6, 7 and 8 given below describe the tolerance $level_2$ calculation with hit count and threshold level. Where ω1, ω2 are fault threshold and correct threshold respectively.

$$+ve \text{ Hit} = \text{Total Hit}(t) - c(t) \quad (4)$$

$$-ve \text{ Hit} = +ve \text{ hit} - f(t) \quad (5)$$

$$\text{Threshold Level 2} = \sum_{i=1}^{n} (\text{Tolerance Level } i - 1, + ve \text{ Hit}) \quad (6)$$

$$\text{Level 2 Outlier Hit} = \sum_{i=1}^{n} \{(\text{Tolerance Level } i - 1, - ve \text{ Hit}) \text{ U } (\text{User\_Access\_Level})\} \quad (7)$$

$$\text{Tolerance Level} = (\text{Threshold Level 2}) \text{ U } (\text{User\_Access\_Level}) \quad (8)$$

4.1.3. Level$_3$

The Q_3 maintains the users who have the high tolerance level at $level_1$ and $level_2$, and, can interact with the online transaction application *i.e.*, third party payment page. Here the tolerance level is fixed based on the time limit in the web interaction. There are two types of order processing namely zero and non-zero order selection. In zero order selection the user simply performs the selection over the web page which will never reflect any changes in the online transaction. This type of selection done by the user will get the session time out as soon as the time gets expired. The non-zero order processing is placed based on Q_1 and Q_2 tolerance level with time limit. If the time gets elapsed the tolerance level is extended to some level which maintains the current session for completing the current transaction. The tolerance $level_3$ is very vital because the online transaction processing gets completed in this stage. The equation 9 and 10 describes the threshold level and final tolerance level of the proposed technique.

$$\text{Threshold Level 3} = \sum(\text{Order\_Processing}(t)) + \sum \text{Selection}(t) + \{\sum \text{Fault}(t) + \text{delay}(t)\} \quad (9)$$

$$\text{Tolerance Level Final} = \{(\text{Tolerance Level 2}) \text{ U } (\text{Threshold Level 3})\} \quad (10)$$

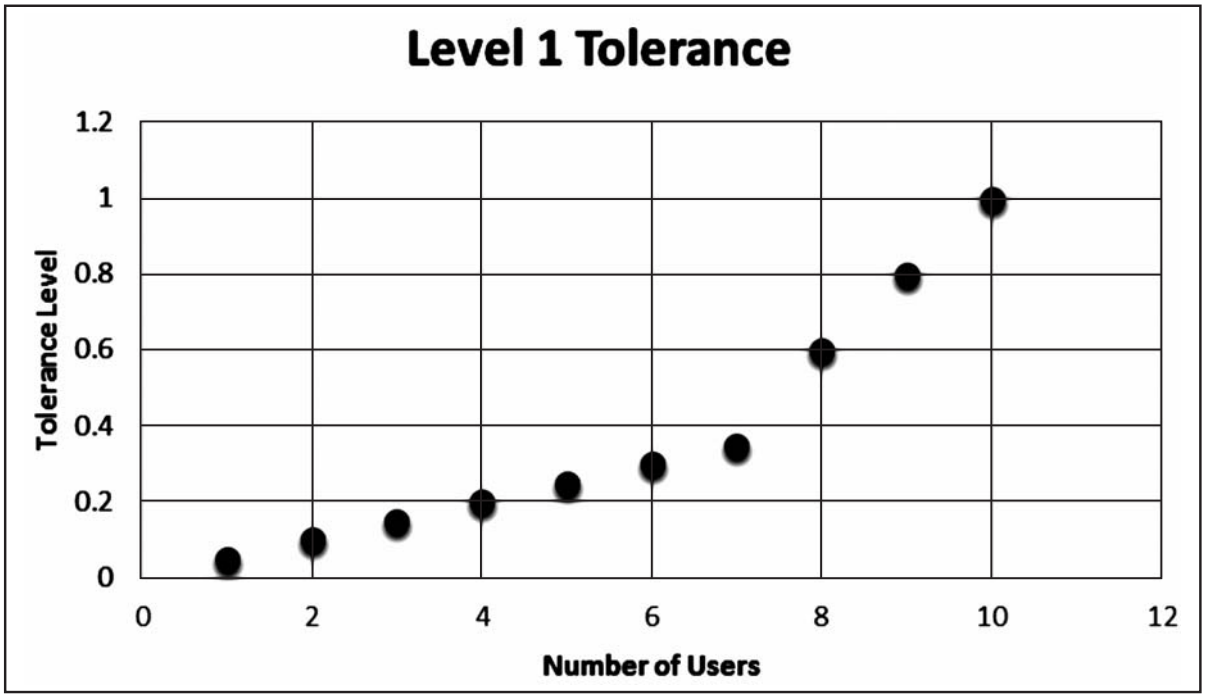

Figure 8: Level 1 Tolerance Comparison

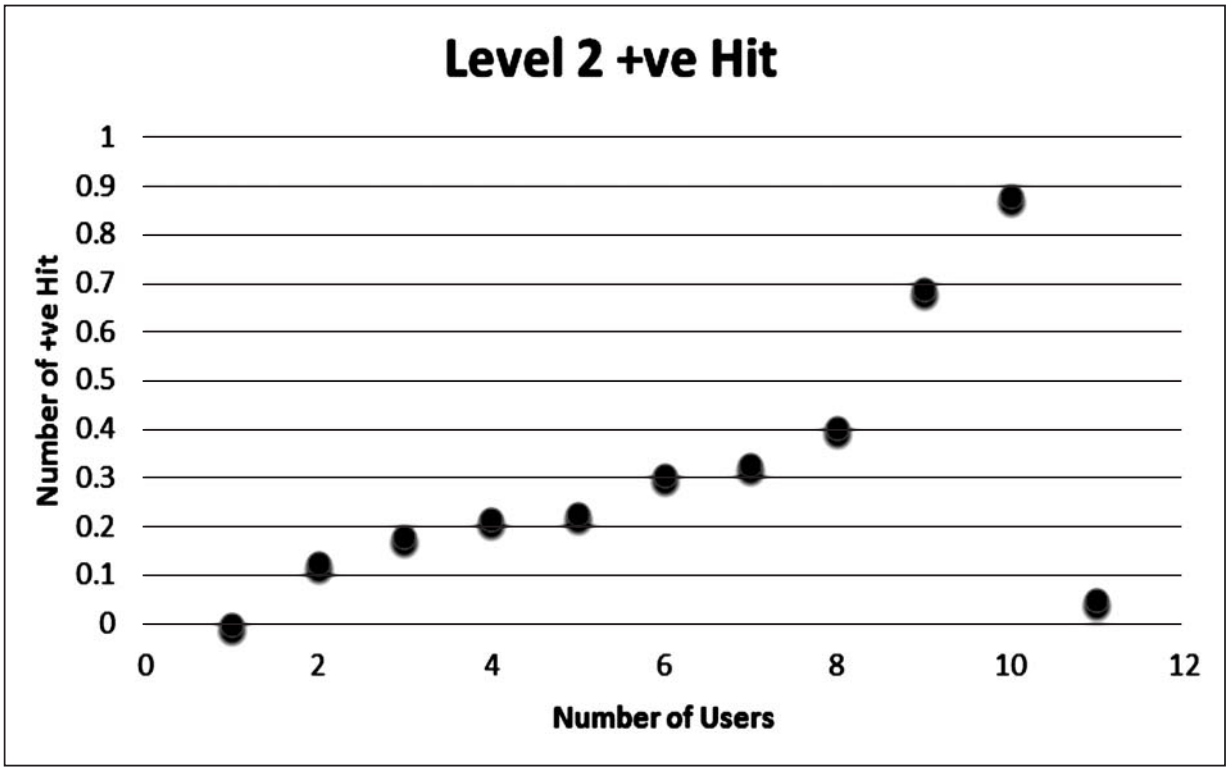

Figure 9: Level 2 Positive Hit Comparison

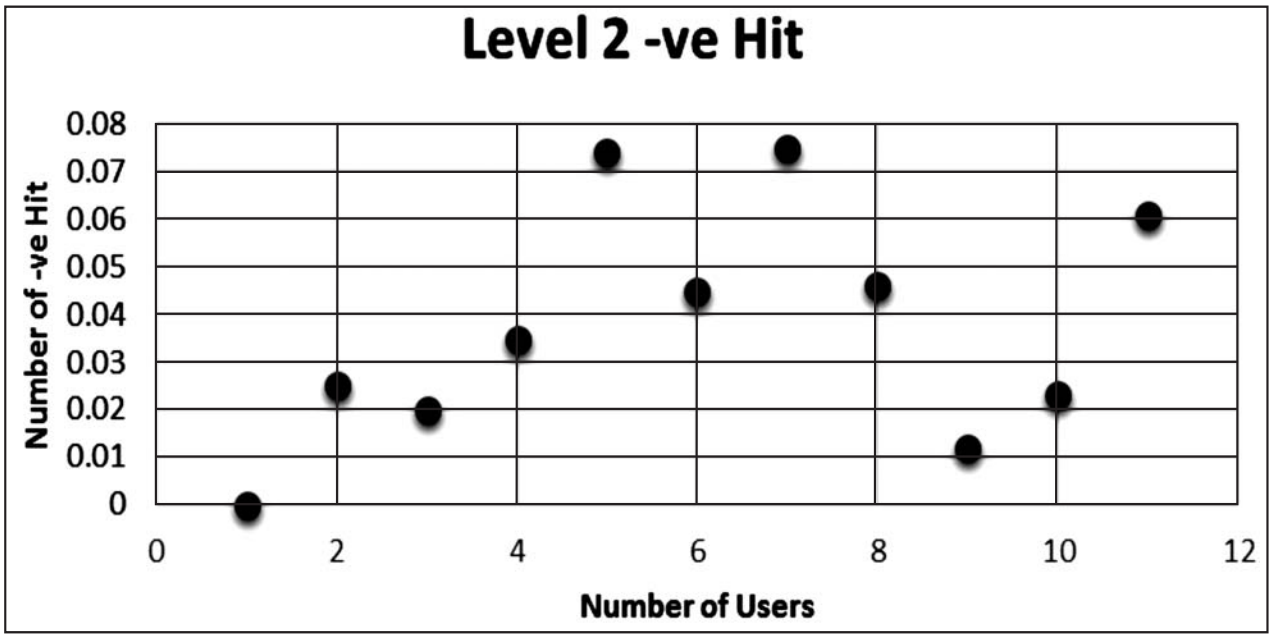

Figure 10: Level 2 Negative Hit Comparison

5. CONCLUSION

To conclude, the error-tolerant design, Risk tolerance and RFM scheme put together, provides a way for genuine customers that make honest mistakes and/or users impacted by external factors (network unavailability) to avoid being hassled and get on with their task by allowing them to recover from error. Undoubtedly this would help reinforce a positive user experience and potentially help business recover potentially lost transactions and contribute to the bottom-line.

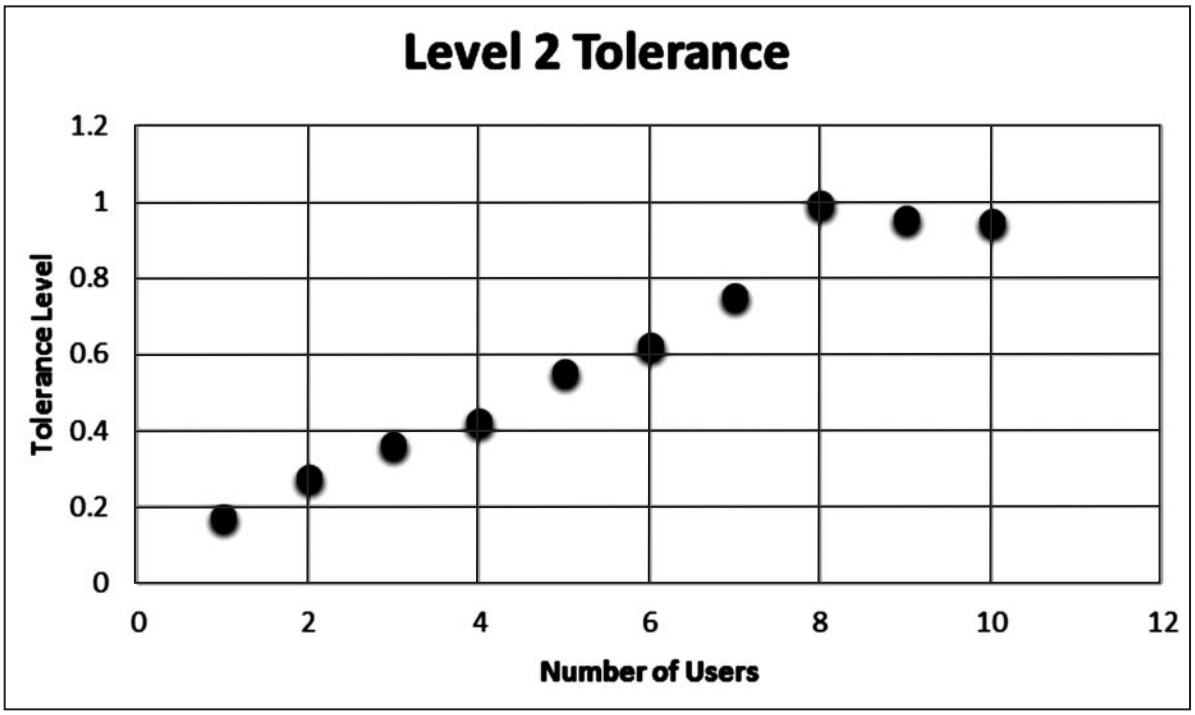

Figure 11: Level 2 Tolernace Comparison

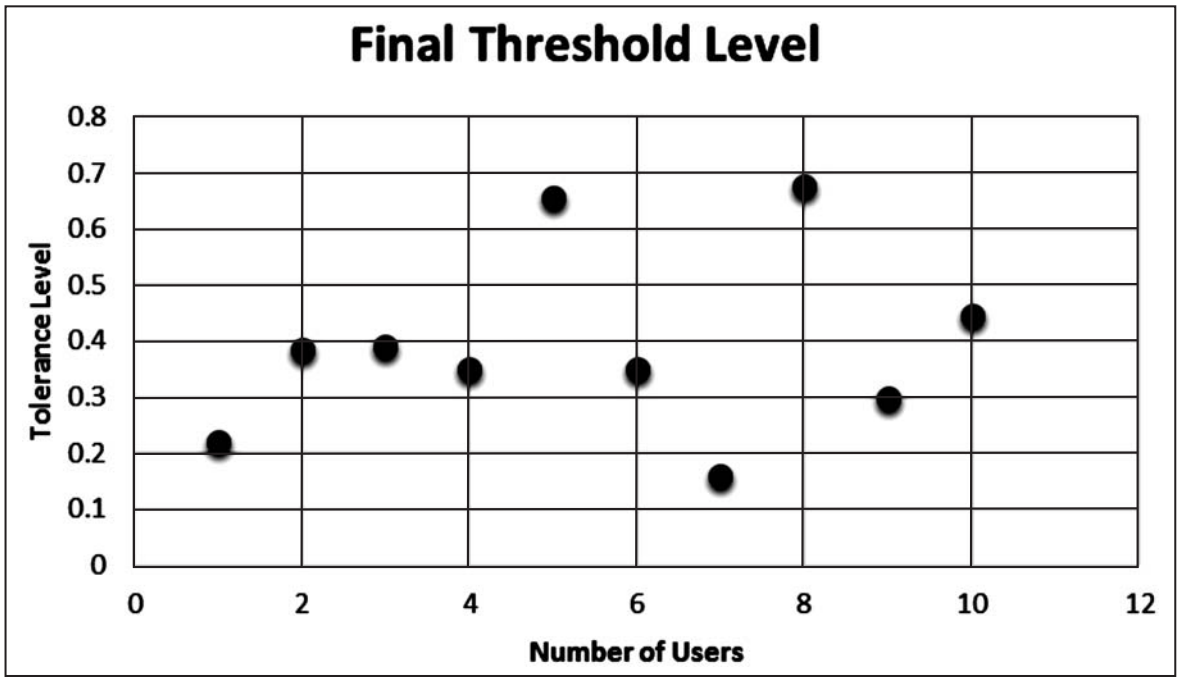

Figure 12: Final (Sensitive) Threshold Comparison

6. REFERENCES

1. G. Robert Redinbo,"Wavelet Codes for Algorithm-Based Fault Tolerance Applications" ,IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 7, NO. 3, JULY-SEPTEMBER 2010,Pp 315-328.
2. Cheng-Long Chuang,Yung-Chung Wang, Chien-Hsing Lee, Maw-Yang Liu, Ying-Tung Hsiao, and Joe-Air Jiang,"An Adaptive Routing Algorithm Over Packet Switching Networks for Operation Monitoring of Power Transmission Systems",IEEE TRANSACTIONS ON POWER DELIVERY, VOL. 25, NO. 2, APRIL 2010, Pp 882-890.
3. Rachana Ashok Gupta, Mo-Yuen Chow,"Networked Control System: Overview and Research Trends",IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 57, NO. 7, JULY 2010, Pp 2527-2535.

4. Ozgur Sinanoglu, Mehmet Hakan Karaata, and Bader AlBdaiwi, “An Inherently Stabilizing Algorithm for Node-To-Node Routing over All Shortest Node-Disjoint Paths in Hypercube Networks”,IEEE TRANSACTIONS ON COMPUTERS, VOL. 59, NO. 7, JULY 2010, Pp 995-999.
5. Henrique Moniz,Nuno Ferreira Neves,Miguel Correia and Paulo Verissimo,”RITAS: Services for Randomized Intrusion Tolerance”,IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 8, NO. 1, JANUARY-FEBRUARY 2011, Pp 122-136.
6. Ing-Ray Chen,Anh Phan Speer and Mohamed Eltoweissy,”Adaptive Fault-Tolerant QoS Control Algorithms for Maximizing System Lifetime of Query-Based Wireless Sensor Networks”, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 8, NO. 2, MARCH-APRIL 2011, Pp 161-176.
7. Stanisław Jarecki, Jihye Kim and Gene Tsudik,”Flexible Robust Group Key Agreement”, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 22, NO. 5, MAY 2011,Pp 789-886.
8. Shucheng Yu, Kui Ren and Wenjing Lou, “FDAC: Toward Fine-Grained Distributed Data Access Control in Wireless Sensor Networks”, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 22, NO. 4, APRIL 2011, Pp 673-686.
9. Quyen L.Nguyen and Arun Sood, “A Comparison of Intrusion-Tolerant System Architectures”, IEEE COMPUTER AND RELIABILITY SOCIETIES, ISSN 1540-7993/11/,JULY/AUGUST 2011, Pp 24-31
10. Y. Huang, D. Arsenault, and A. Sood, “Secure, Resilient Computing Clusters: Self-Cleansing Intrusion Tolerance with Hardware Enforced Security (SCIT/HES),” Proceeding of 2nd Internation Conference on Availability, Reliability, and Security (ARES 07), IEEE CS Press, 2007, pp. 343–350.
11. Vadim Drabkin, Roy Friedman, Gabriel Kliot, and Marc Segal,” On Reliable Dissemination in Wireless Ad Hoc Networks”,IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 8, NO. 6, NOVEMBER/DECEMBER 2011,Pp 866-882
12. Augusto Ciuffoletti, “Preventing the Collision of Requests From Slave Clocks in the Precision Time Protocol (PTP)”, IEEE TRANSACTIONS ON INSTRUMENTATION AND MEASUREMENT, VOL. 60, NO. 6, JUNE 2011, Pp 2096-2103
13. Maxwell Young and Raouf Boutaba,”Overcoming Adversaries in Sensor Networks: A Survey of Theoretical Models and Algorithmic Approaches for Tolerating Malicious Interference”,IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 13, NO. 4, FOURTH QUARTER 2011, Pp 617-641
14. Hairong Qi, Xiaorui Wang,Leon M. Tolbert, Fangxing Li,Fang Z. Peng,Peng Ning, and Massoud Amin, “A Resilient Real-Time System Design for a Secure and Reconfigurable Power Grid”, IEEE TRANSACTIONS ON SMART GRID, VOL. 2, NO. 4, DECEMBER 2011, Pp 770-781
15. Erman Ayday and Faramarz Fekri, “An Iterative Algorithm for Trust Management and Adversary Detection for Delay-Tolerant Networks”,IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 11, NO. 9, SEPTEMBER 2012, Pp 1514-1531
16. Roberto Cortinas, Felix C. Freiling, Marjan Ghajar-Azadanlou,Alberto Lafuente, Mikel Larrea, Lucia Draque Penso, and Iratxe Soraluze,”Secure Failure Detection and Consensus in TrustedPals”,IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO. 4, JULY/AUGUST 2012, Pp 610-625.
17. Cluster based Key Management Authentication in Wireless Bio Sensor Network “, ,International Journal of pharma and bio sciences.
18. Chuanjin Jiang, Wanguen Song, “An Online Third Party Payment Framework in E-Commerce”, IEEE INTERNATIONAL CONFERENCE ON ADVANCED COMPUTER CONTROL, JUNE 2010.
19. Valarie A. Zeithaml, A. Parasuraman, &Leonard L.Berry. “Problems and Strategies in Services Marketing”, Journal of Marketing, 1985(49): 33-46
20. Zeithaml,V.A.,Berry,L.&Parasuraman,A. “The behavioural consequences of service quality”, Journal of Marketing, 1996,60(2):31-46.