Journal of Green Engineering (JGE)

Volume-10, Issue-3, March 2020

An Efficient Incident Recovery Based Information Security model Using Fuzzy Rough Sets for Green Business Environment

[1]Vinod Duraivelu,[2] Udaykumar Kamalakannan, [3] Dhinakaran Kumar, [4] Elantamilan Dhathinamoorthy

[1] *Associate Professor, Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, India. E-mail: vinodd.sse@saveetha.com*
[2] *Assistant Professor, Department of Computer Science and Engineering, Bharath Institute of Higher Education and Research, Chennai, India. E-mail: udaywh18@gmailcom*
[3]*Assistant Professor, Department of Computer Science and Engineering, Rajalakshmi Institute of Technology,Chennai, India. E-mail: dhinakaran.k@ritchennai.edu.in*
[4] *Assistant Professor, Department of MCA , Guru Nanak College, Chennai, India . E-mail: elantamilan.ds@gmail.com*

Abstract

The objective of the work is to propose a fuzzy rough set based incident response plan with attack modeling and verification technique encompassing the information assurance in green business environment. Developed or gathered data about the current or past security incidents in business forms are to be recognized for conveying right security systems. The accuracy of the current data and the accentuation of the past data identified with security are officially used to foresee the truth of future data security occurrences in a business situation. The accentuation on different fragments of the data is investigated according to the fuzzy data in regards to the assaults and their effects. The fuzzy result and lament lattices desire and their relative weightages in different event responds action with business forms are quantitatively displayed to take a right choice with the proposed with Time

Journal of Green Engineering, Vol. 10_3, 811–826.

Contiguity Anxious Logic (TCAL) tense validation. The hopeful green security system is distinguished when numerous business forms with various truth factors are teamed up. The intelligent sequent math with its methods is applied to implement the best option of information assurance and its security activity to defend any attack towards business environment.

Keywords: Fuzzy rough set, structured information, Semantic tense logic, Accentuation Security Event, sequent calculus, information Assurance.

1 Introduction

The interpretation and interconnection of rationales in security space is basic to distinguish a sound judgment in the plan and design of component that sets up and gives security by framework designer [1]. The security include displaying with the general thoughts of space and application building is a tree of highlights with include chain of command. The highlights are sorted into three specifically obligatory, discretionary or elective. A security highlight model can be separated into numerous trees, where a foundation of a tree can be referenced from within another as a sub highlights like assaults and measures to forestall them [2]. To choose the best other option, it isn't unexpected to utilize three distinctive derivation types specifically conclusion, enlistment and kidnapping. Derivation is the sort of thinking which ensures genuine end from genuine premises. It is a kind of argumentation from general to specific though the enlistment is a contention from specific to general, which delivers just likely end that should be confirmed by future perception. As per Pierce "Snatching is the procedures of framing illustrative speculation and it is the main consistent activity which presents new thoughts" [3].

The craving for rationales that are able to do normally and straightforwardly catching the significance of articulations in powerful situations, prompted advancement of specific transient and dynamic rationales [4]. The requirement for an alternate rationale that tends to the issues of access to data frameworks and correspondence is indispensable since the current methodologies have chiefly been at the specialized level utilizing scientific methodologies [5]. The proposed interim and vicinity based rationale tends to the consistent network of security occurrences and their outcomes. The inadequate information about the data security area by and large and the present data security status of the association is one of the principle issues in data security hazard the executives [6]. The data security episode is shown by a solitary or a progression of undesirable or unforeseen

data security occasions that have a noteworthy likelihood of trading off business activities and undermining.

The potential assaults on the data resources and the conceivable security options are to be gathered continuously in order to choose the best system. The data security episode can be purposeful and can be caused both by specialized and physical methods [7]. The paper is sorted out as follows: Section II investigates the rationale and illogic that can be applied in the data security space and Section III proposes an Interval Proximity Tense Logic for associating all the causes and outcomes of security occurrences. Segment IV talks about the determination and check of security episodes by IPT Logic and Section V increases the choice by fluffy result and lament grids and Hurwicz rule with its ideal choice of security component. The end gives restriction of the proposed strategy with a degree for future extemporized choice in data security.

2 Sematic Tense Logic in Information Flow

In the semantics of old style rationale, the dynamic idea of the security episode and movement can't be completely investigated to reason the future security procedures with different assault and it is totally conceivable with occurrence reaction plan system[14]. As indicated by Arthur Prior, a period subordinate idea of reality esteems must be applied for the past as well as to the most recent episodes. The transient rationale speaking to a specific interim of time or at any careful purpose of time is to be determined in order to control the tenses in a conventional manner [9].The Linear Temporal Logic and Computation Tree Logic are utilized to catch the various parts of calculation. The semantics of LTL can be characterized utilizing the progression of time with a way quantifier and without presenting a change while the CTL administrator is characterized as for change frameworks. The paper tends to the significant subjective relations dependent on the time interims as well as their vicinity regarding one another. The work proposes Time Contiguity Anxious Logic (TCAL) in which the administrators like previously, in the wake of, during, since and until are in the interim class and administrators like seconds ago, not long previously and soon after are in the closeness classification and now or present, past, future are in the strained classification as shown in table 1.

B_i= before an Event , A_i = after an Event , D_i = during a period, S_i = since a time mark U_i = until a time mark JN_i= Just Now an Event , JB_i = Just before an Event , JA_i = Just after an Event N = now an Event , P= was an Event , F= will be an Event X_i = never an Event , Y_i = always an Event , Z_i =

sometimes an Event as given in Table 1. The classified data is accessible in a tremendous information base, for example, banking division, car industry, etc, where more gatecrashers can clear a path to pulverize or to hack the secret data because of security blemishes in the association [10]. The data might be spilled or duplicated during a specific timeframe. This occurrence may have happened after or before a comparable episode. There might be numerous such security occurrences until the current security systems are fortified.

Table 1. Information Tense Logic Operators

Time Logic		**Contiguity**		**Anxious Logic**	
Symbol	***Sequence***	***Symbol***	***Sequence***	***Symbol***	***Sequence***
B_i	Before an event	JN_i	Just Now an event	N_i	Now an event
A_i	After an event	JB_i	Just before an event	P_i	Was an event
D_i	During a Time period	JA_i	Just after an event	F_i	Will be an event
S_i	since a time spot	X_i	never an event	Z_i	Some time an event
U_i	until a time spot	Y_i	always an event	O_i	Often an event

A period mark is expected to dodge this sort of security occurrences through the transient availability by gatecrashers in any association. Trading off the data misfortune in an association is an immediate capacity of the vicinity of such episodes or recurrence of comparable security ruptures that outcomes some ongoing or late assaults[11]. The counteraction or security move might be made soon after the assault or not long before an occurrence. Now and again the ongoing kind of occurrence may never occurred over an extensive stretch of time in the present section of business or it might be a customary danger causing a similar episode consistently with information domain as shown in figure 1.

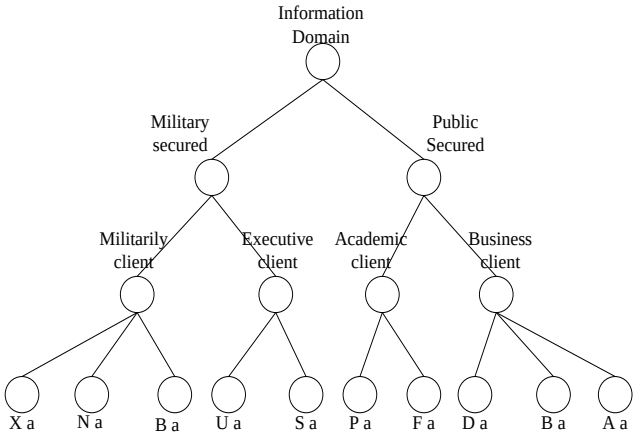

Figure1 Time and Objective Information Security Tree

The ineffectiveness can be recognized and rectified however the consistency of any assault is troublesome[15]. The formal business association may confront comparative security episodes in future as it has encountered in the present and the past. Individuals in general made sure about area manages the scholarly and business customers where greater security defects can be distinguished to unlawful access of data inside and remotely[12]. The assailant can get to the data with regardless time and transmission arrangement. The FOL doesn't permit us to speak to the activity "now" in the main articulation, the activity "after" and "until" in the subsequent proclamation, the activity "after" in the third explanation and the activity "during a period" in the fourth explanation. FOL permits the portrayal of the announcements in an extremely conventional way; it underpins just a set number of explicit conditions without centering the pressing activities and its common sense.

For example in FOL the statement can be represented as,

$[\text{Migrate}\ (V_{A,}\ P_S)\ /\backslash\ \text{File Transfer (Sequence)}] \rightarrow$

$[\sim \text{Change}\ (C_P) \rightarrow \text{Process}(E_R)]\ /\backslash\ \text{Proxy}_s\ (\text{loc1})\ \backslash/\ \text{Proxy}_s\ (\text{loc2})$

Consider the logical statement “If the certificate is hacked or virus attack is comprehended or imposition detection is acknowledged, then do fix it now with flow logic”. Its equivalent First Order Logic (FOL) is given by

$$\exists t\ System(N_C,t) \vee System(V_A,t) \vee System(I_D, t) \longrightarrow fix(System)$$

Where, V_A represents Virus Attack, D_H represents Document Hack, I_D represents Intrusion Detection and t represents time. The above First Order Logic gives a portrayal which says "fix the framework" however neglects to make reference to when the activity of fixing must be performed for example it must be fixed at this point. Think about another announcement "In the event that a framework is under danger, at that point don't associate it to some other system and never share any document through that framework”. Its FOL is given as,

$$\exists s, \exists t\ Threat(s,t) \rightarrow\sim Connect(s,s1)\ \wedge \sim Share(file,s)$$

Where s, s1 represent system and t represents the current time not the future. The above First order Logic implies that the documents must not be common however prematurely delivers the equivalent where express that they ought to never be shared through the framework until the risk is evacuated. Think about another announcement "If a security rupture has happened in the system and the information has undermined in the framework, at that point perform switching after the episode".

$$Security\ Breach\ (Network)\ \wedge\ Data\ (System)\ \longrightarrow Reversing\ (Attack)$$

The FOL representation states that reversing must be performed but it fails to state that it has to be performed “after the event’. The virtual applications (V_A) should be immediately migrated to another physical server (P_S) and then the file transfer should be carried out in the correct sequence as per the order of the business mail. The emergency requests (E_R) during a period should be preserved until the confidentiality policy (C_P) changes when the proxy server is at location1 or location2.

TCA Logic

A Time Contiguity Anxious Logic is proposed along with the existing operators in LTL and CTL.

The Time Logic Grammar can be represented as:

$$\varphi ::= T|i|B\varphi|A\varphi|D\varphi|S\varphi|U\varphi$$

The Contiguity Logic Grammar is given by:

$$\varphi ::= T|i|J.N\varphi|J.B\varphi|J.A\varphi|X\varphi|Y\varphi$$

The Anxious Logic Grammar is defined as follows:

$$\varphi ::= T|i|N\varphi|P\varphi|F\varphi|Z\varphi|O\varphi$$

Where φ represents a set of Event s i $\in \varphi$. T represents a set of time points.

If there should be an occurrence of assaults on a data framework some security activities must be done dependent on the closeness, tense and interim at an example of time when the assault happens. The CTL and LTL can't be utilized to speak to the critical idea of the recuperation activities which might be classified as exercises that ought to be finished as for interim, time, and nearness. The proposed TCAL might be utilized to speak to the energy and wellbeing properties of different activities that are to be taken. Some worldwide framework factors or neighborhood factors are to be kept invariant when quantities of such parts are required the security and the nearby factors are to be checked for their end or right execution for energy property of the framework.

3 TCAL Specification and Verification towards Incident Responds Plan

Specific logics in LTL and CTL are evaluated in time points at a particular state of incident responds with validation on information. A more powerful way of representing temporal logic is with respect to intervals. Only three main relationships can be specified in intervals: before, after and equal[13]. On the other hand Allen's relationship gives thirteen distinct relationships between time intervals which include "overlap", "during" etc… Thus this model can be considered as a collection of intervals with temporal relations between them. Temporal logics are limited to just time varying properties of a domain. In order to address the actions that results in these changes we need to use dynamic logic. This logic is mainly used for a program that is structured and explains their behavior. Hence new operators may be incorporated such that the intensive system can perform some actions based on the decision taken among these sample conditional logics shown in eight sensible steps below.

1. If information leak (I_L) occurs ***just before*** (JB_i) packet capturing (C_p) then progression of integrity policy (I_p) and patterned for the loss of information (L_i). This can be reasonably represented as $JB_i (C_p)$,
$I_L \vdash I_p \wedge L_i$.
2. If there any occurrence in loss of information (L_i) ***always*** (A_i) then excellence of information flow routine is reduced. This can be logically represented as
$L_i \vdash \neg P$.
3. If the performance (P) of the classification is excellent and certainly not a threat (T) happens then security (S) is sustained in the system. This can be reasonably represented as $P \wedge \neg T \vdash S$.
4. If data is modified (M_D) due to inside attacks (I_A) which take place ***often*** (O_i), then patterned confidentiality policy and also allow access control (A_c). This is reasonably represented as
$O_i (I_A), M_D \vdash CO_p, A_c$.
4 Presently the confidentiality policy (CO_P) is reliable ***until*** (U_i) the security service provider's (Sec_{SP}) request for a policy revision (P_R). This is sensibly represented as P_R,

$$Sec_{SP} \vdash \neg CO_p .$$

6. Buffer overflow (B_o) hints to denial of service and it can be sensibly represented as $B_o \vdash JA_i (DOS)$.
7. If data corruption (D_c) chances ***just after*** (JA_i) an Event of denial of service (DOS) then patterned the regulation based privacy policy (R_B) and allow trust managing scheme (T_S). This declaration can be sensibly represented as

$$JA_i (DOS), D_c \vdash R_B, T_S.$$

8. Once the trust management system is empowered, it is prepared sure, at the moment onwards the security is conserved and there is no modification in the application security policy until administrations fix vulnerability (V) in the quartered application.
This is sensibly represented as

$$T_S \vdash N_i (S) \wedge \neg V.$$

Premise1: $JB_i (C_p), I_L \vdash I_p \wedge L_i$

Premise2: $L_i \vdash \neg P$

Premise3: $P \wedge \neg T \vdash S$

Proof:

$JB_i (C_p), I_L \vdash I_p \wedge L_i \wedge 1\varepsilon$

$JB_i (C_p), I_L \vdash L_i \quad L_i \vdash \neg P$ Cut rule

$JB_i (C_p), I_L \vdash \neg P \quad \neg R$

$JB_i(C_p) \vdash \neg P, \neg I_L \neg L$

$JB_i(C_p), P \vdash \neg I_L$ LW

$\neg JB_i(C_p) \wedge JB_i(C_p), P \vdash \neg I_L$

$P \vdash \neg I_L \quad P \wedge \neg T \vdash S$ Cut rule

$P/\backslash \neg T \vdash S, \neg I_L$

Premise4: $O_i(I_A), M_D \vdash CO_p, A_c$
Premise5: $P_R, Sec_{SP} \vdash \neg CO_p$
Proof:

$O_i(I_A), M_D \vdash CO_p, A_c \neg L$

$P_R, Sec_{SP} \vdash \neg CO_p \quad O_i(I_A), M_D, \neg CO_p \vdash A_c$

Cut rule

$P_R, O_i(I_A), M_D, Sec_{SP} \vdash A_c$ RW

$P_R, O_i(I_A), M_D, Sec_{SP} \vdash A_c, S$

$R \Rightarrow O_i(I_A), M_D, Sec_{SP} \vdash P_R \Rightarrow A_c, S$

Premise6: $B_o \vdash JA_i(DOS)$

Premise7: $JA_i(DOS), D_c \vdash R_B, T_S$
Premise8: $T_S \vdash N_i(S) \wedge \neg V$
Proof:

$B_o \vdash JA_i(DOS) \quad JA_i(DOS), D_c \vdash R_B, T_S$ Cut rule

$D_c, B_o \vdash R_B, T_S \quad T_S \vdash N_i(S) \wedge \neg V$ Cut rule

$D_c, B_o \vdash R_B, N_i(S) \wedge \neg V \neg R$

$B_o \vdash \neg D_c, R_B, N_i(S) \wedge \neg V$

4 Fuzzy Decision Making on Information Asset

The security attacks that degrade the systems performance along with their control mechanisms have been discussed in Table2. The best mechanism that will counter the security attacks is chosen from the listed mechanisms using fuzzy pay off matrix method.

Table 2. Fuzzy Rough Set Payoff Based Incident Responds on Attack

Attack on Asset / Incident Responds Plan	Denial of Service	Information Leakage	Sniffing	Session Hijacking	Spoofing	Sniffing	Availability	Virus and Trojans	Internal Attack	Information Overflow
Abnormal Index	1	1.25	2	2.75	3	3.95	0	4	5	6.25
Imposition Detection	4.25	5	10.50	9.60	8.15	7.25	2	6	2.25	5
Session Time stamp	7.45	8.20	5.25	9.50	7.25	6.50	8.25	1.25	2	7
Security Setup	5.50	7.50	8.50	7.50	1.50	5.50	4.50	2.50	7.50	7.50
Information Breach	7.30	4.35	4.45	5.55	3.65	5.75	5.25	4.85	4.95	5.10
Internal Monitoring	7.10	8.20	9.30	7.40	4.50	7.60	3.70	10	9.80	6.90
External Monitoring	8.25	9.30	9.35	7.40	7.50	6.55	5.60	4.65	8.70	5.75
Security	7.05	6.15	7.25	8.35	6.45	8.55	7.65	1.25	9.75	5.80
Trust Ratio	7.20	6.30	5.40	7.50	8.60	4.70	7.80	3.20	5.90	4.95
Highest Payoff	8.55	9.60	10	9.65	9.70	8.75	10	10	9.80	8.85

The fuzzy set is:

S_1=[(1,0.25) (2,0.5) (3,0.875) (4,0.65) (5,0.7) (6,0.35) (7,0.15) (8,0.1) (9,0.475) (10,0.55)]

The fuzzy pay off is calculated as follows:

P_1= [(0.250,5) (0.5,6) (0.875,7) (0.65,8) (0.7,9) (0.35,3) (0.15,10) (0.1,2) (0.475,1) (0.55,8)]

Similarly,

P_9=[(0.25,7) (0.5,6) (0.875,5) (0.65,7) (0.7,8) (0.35,4) (0.15,7) (0.1,3) (0.475,5) (0.55,4)]

$P_{max} = SUP_x(X) = 10$

XM_1 = [(0.5,5) (0.6,6) (0.7,7) (0.8,8) (0.9,9) (1,10) (0.3,3) (0.2,2) (0.1,1) (0.8,8)]

Similarly,

XM_9 = [(0.7,7) (0.6,6) (0.5,5) (0.7,7) (0.8,8) (0.4,4) (0.7,7) (0.3,3) (0.5,5) (0.4,4)]

PS_9= [(0.250,5) (0.5,6) (0.7,7) (0.65,8) (0.7,9) (0.3,3) (1,10) (0.1,2) (0.1,1) (0.55,8)]

Finally,

The Hurwicz value, when a=0.5

$Hv_i = a\ Hf_{ai} + (1-a)\ Lf_{ai}$

.5(0.7,0.875,0.7,0.8,0.5,0.875,0.9,0.9,0.8)+0.5(0.1,0.1,0.1,0.1,0.1,0.1,0.4,0.1, 0.3)

Hv_i=(0.4,0.48,0.4,0.45,0.30,0.48,0.75,0.50,0.55)

The largest value is 0.75 with respect to event security representation with fuzzy payoffs with respect to basic scenario which has been verified with the fuzzy payoff as shown in figure 2, and it is obtained for Trust analysis in organizations information asset. Hence this is taken as the best mechanism to provide a highest payoff matrix to prevent attacker's scenario for any future attacks and its representation internally or externally.

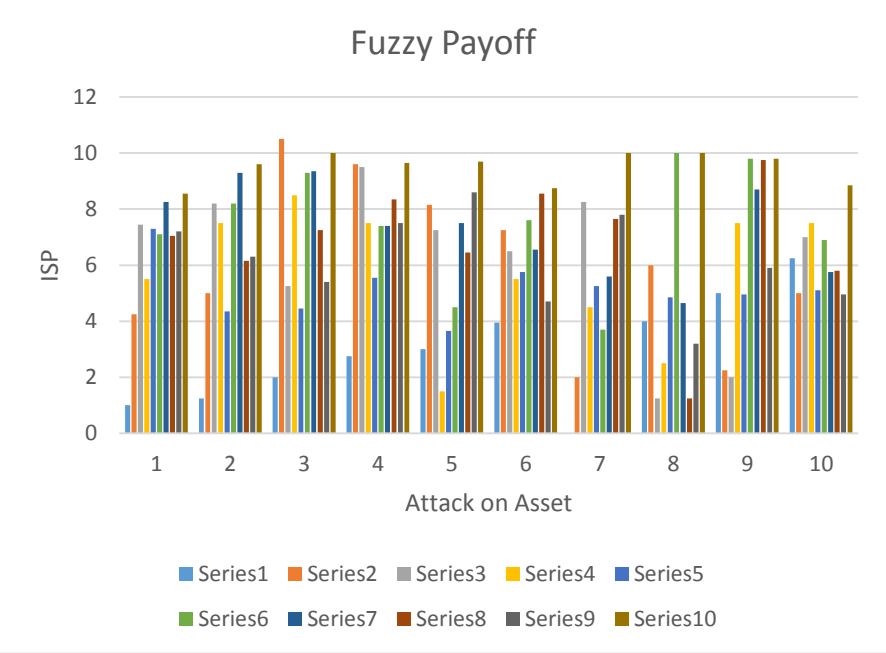

Figure 2. ISP towards Attack on Asset Payoff

5 Conclusion

The time contiguity anxious logic is proposed for indicating the security Event s and systems and utilizing the fluffy dynamic methodology, the best security component is distinguished. The fluffy result grid and the Hurwicz rule enlarge the choice for any security space with various classes of customers. The assaults and their required security activities as well as their outcomes are checked utilizing sequent math. The system checking component is distinguished as the hopeful methodology when contrasted and a quantities of safety efforts. The feeble point in the proposed approach is the absence of space or system explicit instruments and their relative weight components or information in security area. The other territory where the proposed procedure might be additionally tuned by various time fluctuating security arrangements of the association .The future work focuses on the security rationale expected to teach the reasonability and relocation highlights of the basic data between various systems. The type2 fluffy

rationale will be applied to cover most extreme vulnerabilities in the security Events and assault data to precisely choose the most ideal static security arrangement or procedure for business association.

Reference

[1] Vinod. D, A. Saritha arumugam, "A Framework and Assessment of Information Security in the Product Design Centre: A Quantifiable Analysis on Information Flow" International Journal of Engineering and Advanced Technology, Vol.9 ,no.1, October 2019.

[2] Kiran Kumar, Vinod. D, "An Improved Prediction on Consumer Purchase Intension Using Social Media Data's using Machine Learning" International Journal of TEST Engineering and Management, Vol.82 no.1, February 2020.

[3] Sivanesh kumar. A, "Logics and Illogic's in Information Security Flow on Process Development Environment" International Journal of Innovative Technology and Exploring Engineering (IJITEE), Vol.8, no.11S, September 2019.

[4] Vinod.D, "An Intangible Information Security Frame Work Against Attacks in Business Environment" International Journal of Innovative Technology and Exploring Engineering (IJITEE), Vol.8, no.11S, September 2019.

[5] Sabater, J. and Sierra, C, "A reputation model for gregarious societies". In: Proc of the 4th workshop on deception fraud and trust in agent societies, Vol.7, pp. 61-70, 2001.

[6] Shebaro, B, Sultana, S, Gopavaram, SR and Bertino, "Demonstrating a lightweight data provenance for sensor net-works", in Proceedings ACM Conference Computer Communication Security, pp. 1022-1024, 2012.

[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 ScienceandTechnology, Vol. No. 4,pp. 95-105, 2014

[8] Trbovich, P.L. and Patrick, A.S., "The impact of context upon trust formation in ambient societies", Workshop on Considering Trust in Ambient Societies, Vienna, Austria, Vol. 16, pp. 26-36, 2004.

[9] Vaiman, M, Bell, K, Chen, Y, Chowdhury, B, Dobson, I and Hines, P, "Risk assessment of cascading outages: Methodologies and challenges," IEEE Transactions on Power System, Vol. 27, No. 2, pp. 631–641, 2012.

[10] Wang, K, Wu, M and Shen, S, "Secure Trust-Based Cooperative Communications in Wireless Multi-hop Networks", Communications And Networking, Book chapter 18, Book edited by: Jun Peng, , pp. 360-378, 2010.

[11]Mc Cormac, A., Parsons, K. M., Butavicius, M. A. "Preventing And profiling malicious insider threats" (DSTO Technical Report,DSTO-Canberra, Australia: Defence Science and Technology Organization.TR-2012-2697, 2010.

[12] Mosier, K. L., Fischer, U, "The role of affect in naturalistic decision Making". Journal of Cognitive Engineering and Decision Making, Vol.4,no. 3, pp.240-255, 2011.

[13] W. Su, S. J. Lee, and M. Gerla, "Mobility prediction and routing in ad-Hoc wireless networks," Int. J. Netw. Manage .IEEE transaction, vol. 11,No. 1, pp. 3–30, 2017.

[14] R. Dube, C. D. Rais, K. Y. Wang, and S. K. Tipathi, "Signal Stability based adaptive routing (SSA) for ad hoc mobile networks," IEEE Papers Commun., vol. 4, no. 1, pp. 598-598, 2015.

[15] K. Du, Y. Yang, A qos routing for maximum bandwidth in ad hocNetworks, in: ICFN '10: Proceedings of the 2010 Second International Conference on Future Networks, IEEE Computer Society, Washington, DC, USA, pp. 343–345, 2010.

Biographies

Vinod Duraivelu was born in Chennai, Tamil Nadu, and 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, and 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, and India in 2009. And he completed his doctor of philosophy in information security at Sathyabama University, Chennai, Tamil Nadu, and India 2018. He presently working as an associate professor and the Research Group Head at Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, Tamil Nadu, India

since 2019. His current research is focusing on information security architecture and information flow control in machine learning environment.

Udayakumar Kamalakannan was born in Chennai, Tamil Nadu, and India in 1983. He completed his under graduate degree in Bachelor of Engineering -Computer Science and Engineering with First Class at Anna University, Chennai, Tamil Nadu, and India in 2005. And he completed his post graduate degree in Master of Engineering in Computer Science and Engineering with First class at Anna University, Chennai, Tamil Nadu, and India in 2009. He presently is working as an Assistant Professor at Bharath Institute of Science and Technology, Bharath Institute of Higher Education and Research, Chennai, Tamil Nadu, India since 2020. His current research is focusing on information security architecture and Big Data Analytics in machine learning environment.

Dhinakaran Kumar received his B.E Computer Science and Engineering from Sri Ramanujar Engineering College,Anna University ,Chennai in 2011, Master of Engineering in Computer science and Engineering in 2013 from Sri Venkateswara College of Engineering, Anna University and pursuing Ph. D in Anna University, Chennai, Tamilnadu, India from 2018. He is currently working as an Assistant Professor in the Department of Computer

science and Engineering at Rajalakshmi Institute of Technology with total teaching experience of 7 years. He has been actively doing research in the area of Cloud computing, Data analytics and data security.

Elantamilan Dhatchinamoorthy was born in Ariyalur, Tamil Nadu, and India in 1982. He completed his Under Graduate Degree in Bachelor of science in Computer Science with First Class at Bharathidhasan University, Trichy, Tamil Nadu, and India in 2004. And he completed his post graduate degree in Master of Computer Application with First class with Distinction at SRM University, Chennai, Tamil Nadu, and India in 2007. And he completed his doctor of philosophy in Image Processing & Artificial Neural Network,Dr. MGR Educational and Research Institute University, Chennai, Tamil Nadu, and India 2018. He presently working as Assistant professor in Department of MCA,Guru Nanak College, Chennai, Tamil Nadu, India since 2019. His current research is focusing on information security architecture and information flow control in machine learning environment.