International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 6, No.2 (Mar-2017)
http://dx.doi.org/10.12785/ijcds/060204

Fuzzy STRIDE Model based on Werners Aggregation Operator for Computer Network Threat Modelling

Salman A. Khan

Computer Engineering Department, University of Bahrain, Sakhir, Bahrain

Received 21 Nov. 2016, Revised 21 Dec. 2016, Accepted 23 Jan. 2017, Published 1 Mar. 2017

Abstract: Security has become a significant concern in proper functioning of modern network systems. To prevent and mitigate a system from attacks, an important issue is realization of the possible damage that different threats could cause to a network system. Keeping this issue in view, this paper proposes modeling of threats and their risk assessment. The STRIDE threat assessment model covers numerous existing threats that are related to all security properties necessary for a secure network. A STRIDE based strategy has been proposed which takes the number and types of attacks as input and applies a fuzzy logic based threat assessment approach to assess the level of attack. The presented work uses a fuzzy operator, namely, Werners operator and a decision-making approach based on a fuzzy rule. KDD 99 dataset was used to evaluate the proposed fuzzy STRIDE model. Empirical results indicate that the proposed approach was able to identify the combined threat level of multiple types of attacks.

Keywords: Network Security, Automated decision-making, Fuzzy logic, STRIDE

1. INTRODUCTION

One of the major concerns in modern computer networks is security from internal and external threats. Enterprises all over the globe suffer from huge financial losses due to network security breaches where different attacks affect network assets. These assets include important and confidential information, as well as network hardware and software resources. Therefore, it is of utmost importance to develop and maintain a secure network for protection of assets. Computer or network security strives to detect and prevent illegitimate and unauthorized use of hosts and networks. This signifies the fact that a secure network should provide confidentiality, integrity, authentication, non-repudiation, and availability to all legitimate users [1]. In a well-structured network, a three-level security strategy is adopted, comprising of the following steps [2]:

1. Prevention, which is concerned with stopping an attack from succeeding.

2. Detection, where an attack is detected and the network administrator is informed about the attack.

3. Mitigation, which entails the ability to minimize loss and recovery from the attack.

It is of utmost importance to analyze the risk a network could be exposed to, before developing a secure network. That is, it is essential to know the possible impact of damage to a system by an attack. The probable threats must be identified, and it must be determined as which dimension of security would be violated by a certain attack, prior to establishing a network. There are various ways to identify and prioritize threats. The process of recognizing, measuring, and investigating potential threats of a system is known as Threat Modeling [3]. Threat modelling is concerned with identifying the possible threats and rating them based on their level of risk. Threat modeling is done to comprehend the level of any attack (high, moderate, low etc.). Such levels can aid in the mitigation strategies.

The selection of an appropriate threat model is based on two distinct, yet related factors. First is the description of security issues that the designer cares about. Second is based on security aspects, i.e. by just looking at a software or program one can easily define the set of possible attacks to categorize [4]. This categorization of threats stipulates a structured approach for systematic identification of threats. Many threat models like STRIDE, DREAD, SWOT, and OCTAVE have been developed for various functions [1]. Among these models, the STRIDE model is adopted in many network systems

E-mail: sakhan@uob.edu.bh

due to its comprehensiveness, and therefore provides a motivation to be the base threat model in this paper.

STIRDE is an abbreviation for **S**poofing, **T**ampering, **R**epudiation, **I**nformation disclosure, **D**enial-of-service, and **E**levation of privileges. The model was developed by Microsoft for categorizing threats [4]. The categorization of threats in this model is done by classifying the nature of exploitation done by attacker or intruder. Furthermore, because it covers numerous attacks and is a simpler yet comprehensive approach for threat identification, it is the best method to generate the threat level. The STRIDE approach gives a clear direction towards forming a model which covers almost all the possible threats which may occur to a network or computer.

The STRIDE model, where each threat is unique in itself, cannot be analyzed using binary logic due to uncertainties involved in the attack detection process. Therefore, a desperate requirement of an analytical approach arises that could integrate the complexity of such threats and construct tailored solutions [5]. Fuzzy logic answers the call, since it has the potential of merging human knowledge into technical (computer based) decision making. In this paper, fuzzy logic works in a way that crisp inputs are taken as the number of threats which outputs the level of attack.

The rest of the paper is organized as follows. Section 2 presents a brief overview of the STRIDE model. Section 3 motivates the use of fuzzy logic in multi-criteria decision-making which forms the basis of the research carried out in this paper. Section 4 discussed the proposed fuzzy logic based STIRDE model. This followed by a short discussion as how the STRIDE model is mapped to KDD99 dataset. The results are discussed in Section 5. Finally, a conclusion is given in Section 6.

2. STRIDE MODEL

A potential violation of the security of a system or a network is called a threat [6]. This may lead to loss of data, or access to data by unauthorized person etc. This implies that certain criteria must be followed when developing a secure network. To counter different types of threats, modes of security have been divided into following five categories [7].

- Integrity - To assure that data has not been altered illegally
- Availability - Continuous presence of a service or resource
- Confidentiality - To safeguard information from revelation
- Authenticity - Ability to legalize a resource along with data
- Accountability - Skill to confidently relate specific incident to a particular entity

With the consideration of the aforementioned issues, Microsoft introduced a threat model referred to as STRIDE which covers all major network attacks. The model is used for different issues related to network security such as identifying threats, dealing with threats and taking appropriate steps to prevent, detect, and mitigate various attacks. Below, a brief discussion of each threat in the STRIDE model is given

A. Spoofing

Spoofing or "Identity spoofing" refers to a scenario in which a user X pretends to be a user Y by changing its identity and gains an illegal access to data resource. This may result in vulnerabilities. Therefore, it is essential that the network authenticates the user's identity. Thus, spoofing can be managed through authentication property [8].

B. Tampering

As the name implies, tampering refers to change of data by an illegal person who is not authorized to modify it. If packets sent by a user over a network are tampered, it would result in affecting the integrity of the system [4]. Thus, the integrity can be maintained by blocking an unaccredited user from manipulating the data. The system needs to examine data received from any user and confirm that the message received by the user has not been altered.

C. Repudiation

This category relies on the fact that a security system must always be able to trace the entity responsible for any illegitimate modification and illegal access of resource or account. This is known as the non- repudiating act of any network. In contrast, repudiation is the situation where any user does not agree on performing an act and is not able to identify the one who did this illegally, such as sending an email, transaction of money etc. Due to these reasons there is a need of auditing and keeping record of all the activities over a network [6]. Users may dispute transactions if there is insufficiency in these needs. This falls under the property of accountability. Thus, repudiation takes care of the fact that the user cannot deny after performing an act [2]. STRIDE takes care of the "masquerading attack" where intruder gains illegal access to personal data through a valid user's identification using fake identity [10].

D. Information Disclosure

Information disclosure assists an attacker or malicious user in achieving confidential information for which he is not permitted. Users are fairly cautious of submitting private details to a system or other user through network. Personal details, bank account details or business details are meant to be confidential for the users which mean that only the intended person should be able to see and utilize that data [11]. To safeguard such sensitive data from leakage, the confidentiality of data must be maintained [4]. STRIDE is capable to responding to the following types of information disclosure.

E. Denial of Service

Denial-of-service (DoS) attack is an attempt to disturb a resource, network, or system in such a way that the intended and valid user wouldn't be able to use it. The attackers usually do this through blocking the network by sending infinite packets over the network [12]. This blocking can be done at the destination, communication channel or by discarding messages between sender and receiver. In order to prevent such attacks the network security is responsible to ensure that the system or resource is always available to the valid users. Following DoS attack types are handled by STRIDE.

F. Elevation of Privilege

Elevation of privilege is the category of attacks in which the intruder gets the authorization more than what has been granted originally. This means that any user is not admitted to elevate his privilege to a higher level on his own. Concerning the authorization property of network security, it is very important to guarantee that solitary the legalized roles can access restricted functionality [8].

3. Fuzzy Logic and Multi-criteria Decision Making

Fuzzy logic was initially proposed by Zadeh in 1965 [9]. Although the fuzzy logic approach did not receive attention initially, the logic has found significant applications in a variety of areas in the last four decades.

One notable application of fuzzy logic is in the area of multi-criteria decision making (MCDM). MCDM is a technique used in scenarios where decisions need to be made in presence of multiple and conflicting criteria. MCDM is concerned with decisions about selecting the best choice from a finite set of available alternatives. The presence of multiple criteria triggers a number of issues involved with MCDM. In majority of problems, the issue of data incommensurability is encountered. That is, the data comes in different units and magnitudes and therefore cannot be combined together in a raw form. Furthermore, the preference of criteria over one another is often desired by the decision maker. Various approaches have been proposed to deal with these two issues. Fuzzy logic is one such approach that has been effectively employed to solve a variety of MCDM problems. Another major motive to consider fuzzy logic for MCDM problems is that fuzzy logic is capable of handling uncertainties in design data.

To deal with MCDM problems using fuzzy logic, criteria are aggregated to form an overall decision function which is scalar value. An important issue here is the selection of a suitable decision function, since there are a wide variety of fuzzy functions available. Usually, the objective in MCDM problems is to satisfy all criteria simultaneously, resulting in the "pure ANDing" operation. There is another form of criteria satisfaction which is known as "pure ORing" where the objective is to satisfy any one of the various criteria involved in the decision process. Most real-world applications are modelled with ANDing approach. However, the pure ANDing operation is traditionally represented as the "Min" function, as defined by Zadeh. In mathematical terms, this representation is very rigid, since it ignores the positive effect of the higher quality criteria and only considers the effect of the lower quality criteria. This issue has led to the development of various other mathematical representations of ANDing operation which are commonly known as soft-AND operators. These operators consider the effect of all criteria equally. One such operator is the Werners' operator [14][15]. The operator is mathematically represented as

$$Y(\mu_A, \mu_B) = \beta \times \min\{\mu_A, \mu_B\} + (1-\beta) \times \frac{1}{2}(\mu_A + \mu_B), \quad 0 \le \beta \le 1$$

where μ_A and μ_B represent the membership value of the first and second decision criteria, respectively. Moreover, $Y(\mu_A, \mu_B)$ corresponds to the membership value of the overall decision function. Further details and mathematical properties of the Werners' operator are given in cane be found in [14][15].

4. Fuzzy Logic Based Multi-criteria STIRDE Threat Detection Approach

Threat detection with STIRDE requires a multi-dimensional strategy due to a huge variety of attacks to be dealt with. This motivates the need of having a detection scheme that would be capable of dealing with all threats covered by STRIDE. In other words, the scheme should be able to handle all six categories of threats. This signifies that the STRIDE threat detection scheme can be formulated as a multi-criteria decision-making scheme. The function of such a threat detection system would be to identify a single attack or stream of attacks on the network, where the system would raise an alarm based on the intensity and type of attack, whether wired or wireless networks [17].

The proposed system would require three main steps, as enumerated below.

1. Fuzzifying each threat by defining its fuzzy membership function
2. Aggregating each fuzzified threat into a single decision function
3. Interpreting the results of the Step 2 and taking necessary action accordingly.

Each step of the proposed strategy is explained below.

A. Fuzzification of the threats

In this step, each of the six threats are fuzzified. This requires mapping the actual number of attacks into a fuzzy membership range. To define a membership function, the upper and lower bounds for each threat type are needed. In this paper, the following ranges have been assumed for

each threat type. These ranges have been derived based on the available information [3][4][12][13][16][17][18].

Spoofing – (0 – 10)

Tampering – (0 – 10)

Repudiation – (0 – 5)

Information Disclosure – (0 – 5)

Denial of Service – (0 – 10)

Elevation of privilege – (0 – 5)

The membership functions are defined as follows. Note that linear representations are used to define each membership function.

The membership function for Spoofing is formed by using the two extreme values (upper and lower bounds) . The two limits , SMin and SMax, are as mentioned above (0 and 10 respectively). The membership function for Spoofing,$\mu_S(x)$ is mathematically represented as follows.

$$\mu_S(x) = \begin{cases} 1 & \text{if Spoofing}(x) \geq \text{SMax} \\ \frac{\text{Spoofing}(x)-\text{SMin}}{\text{SMax}-\text{SMin}} & \text{if SMin} \leq \text{Spoofing}(x) < \text{SMax} \\ 0 & \text{if Spoofing}(x) < \text{SMin} \end{cases} \quad (1)$$

The membership function for Tampering is formed by using the upper and lower bounds which are TMax = 10 and TMin = 0 respectively. The membership function for Tampering, $\mu_T(x)$, is mathematically represented as follows.

$$\boldsymbol{\mu_E(x)} = \begin{cases} 1 & if\ \ Tampering(x) \geq TMax \\ \frac{Tampering(x)-TMin}{TMax-TMin} & if\ \ TMin \leq Tampering(x) < TMax \\ 0 & if\ \ Tampering(x) < TMin \end{cases} \quad (2)$$

Similarly, the membership function for Repudiation can be formed as follows. The two bounds for repudiation are determined first, using the collected data. Equation (3) represents the membership function, $\mu_R(x)$, for Repudiation. In this equation, RMax =5 and RMin = 0 correspond to the upper and lower bounds, respectively.

$$\mu_R(x) = \begin{cases} 1 & if\ \ Repudiation(x) \geq RMax \\ \frac{Repudiation(x)-RMin}{RMax-RMin} & if\ \ RMin \leq Repudiation(x) < RMax \\ 0 & if\ \ Repudiation(x) < RMin \end{cases} \quad (3)$$

The membership function for Information Disclosure can be formed in the same manner. The upper and lower bounds are taken from the data range where the upper limit IMax = 5 and IMin = 0. The membership function $\mu_I(x)$ will be as follows.

$$\mu_R(x) = \begin{cases} 1 & if\ \ InfoDisc(x) \geq IMax \\ \frac{InfoDisc(x)-IMin}{IMax-IMin} & if\ \ IMin \leq InfoDisc(x) < IMax \\ 0 & if\ \ InfoDisc(x) < IMin \end{cases} \quad (4)$$

With respect to the membership function for Denial of Service, the upper bound DMax = 10 and the lower bound DMin = 0. The membership function $\mu_D(x)$, is defined as given in Equation (5).

$$\mu_D(x) = \begin{cases} 1 & \text{if DoS}(x) \geq \text{DMax} \\ \frac{\text{DoS}(x)-\text{DMin}}{\text{DMax}-\text{DMin}} & \text{if DMin} \leq \text{DoS}(x) < \text{DMax} \\ 0 & \text{if DoS}(x) < \text{DMin} \end{cases} \quad (5)$$

Finally, Elevation of Privileges can have a membership function as given in Equation (6). In this equation, upper limit EMax = 5 and lower limit EMin = 0.

$$\mu_E(x) = \begin{cases} 1 & \text{if EoP}(x) \geq \text{EMax} \\ \frac{\text{EoP}(x)-\text{EMin}}{\text{EMax}-\text{EMin}} & \text{if EMin} \leq \text{EoP}(x) < \text{EMax} \\ 0 & \text{if EoP}(x) < \text{EMin} \end{cases} \quad (6)$$

B. Aggregation of membership functions

After all membership functions are found, the next step is to aggregate all into one decision function. This decision function can be stated as fuzzy rule as follows:

Rule 1: "IF spoofing is low AND tampering is low AND repudiation is low AND information disclosure is low AND denial of service is low AND elevation of privilege is low then the attack is low"

The above rule indicates the conditions which would classify the level of attack. The above rule can be implemented as a t-norm in mathematical terms using the Werners' operator as follows

$$f(x) = \beta \cdot \max(\mu_S, \mu_T, \mu_R, \mu_I, \mu_D, \mu_E) + \frac{(1-\beta)}{6}(\mu_S + \mu_T + \mu_R + \mu_I + \mu_D + \mu_E) \quad (7)$$

In the above equation, *f(x)* represents the overall decision function. This overall decision function signifies the level of attack on the network. Note that the value of *f(x)* is in the range of [0,1]. The nearer the value of *f(x)* to 1, the higher is the level of attack, whereas a low value of *f(x)* indicates a low level of attack.

C. Interpretation of decision rule

The final step is the generation of the threat levels based on the threat rule. For the sake of this paper, three parameters are defined to detect threat level i.e. 'Low', 'Moderate' and 'High'. Again, these levels and their corresponding ranges are flexible and can be adjusted by the security administrator as desired.

Recall that *f(x)* represents the output of the Werners operator. Thus, the ranges are defined as follows.

For $0 < f(x) < 0.3$ the threat level is 'Low'

For $0.3 < f(x) < 0.5$ the threat level is 'Moderate'

For $f(x) > 0.5$ the threat level is 'High'

5. MAPPING OF KDD99 ATTACKS TO STRIDE MODEL

KDD99 [16] is a benchmark test suite exclusively developed for the studies concerning network attacks and security. The dataset contains 500,000 entries consisting of different types of network attacks as well as normal connections (connections showing no attack). As mentioned in column 1 of Table I, there are a total of 35 attacks is KDD99, and each attack is classified into a specific attack category of KDD99 as mentioned in column 2 of the table. Each attack type is classified based on 41 unique features whose values decide about the type of a specific attack. One important task of this paper is to map the attacks of KDD99 to STRIDE model which results in the information given in column 3 of Table I. According to this table, there are five attacks classified as Spoofing, four classified as Tampering, five classified as Repudiation, seven identified as Information Disclosure, seven identified as Elevation of privileges, and seven identified as Denial of Service. Due to the huge size and random nature of attack occurrence in KDD99 dataset, a classifier program was developed which could classify the different attack types and their frequency of occurrence in the dataset.

6. RESULTS AND DISCUSSION

The proposed system was tested on 10 different samples collected randomly from the KDD99 data set. These samples contained different types of attacks as well as normal connections. Each sample consisted of 45 entries containing attacks with different frequencies of their occurrence as well as normal connections. Table II provides the frequency of occurrence and types of these attacks according to STRIDE model. Moreover, Table III provides the corresponding individual membership function for each attack type, the overall membership value using the Werners operator, and the level of attack (high, medium, low) as per the definitions given in Section 4.

As observed in Table III, most attacks are classified as high, with some being moderate or low. There are certain interesting observations in the table. For example, both Attack 1 and Attack 2 result in the same overall membership value of 0.44 which indicates that they both have the same intensity of attacks, despite that fact that Attack 1 has a total of 7 attacks while Attack 2 has a total of 9 attacks. However, the nature of attacks in both is different.

Another interesting situation is with respect to Attacks 4, 7 and 9 which have the same number of attacks (17 attacks) as observed in Table II. However, the level of intensity as specified by the overall membership value is different. For Attack 4, the overall membership value is 0.55 while for Attack 9, the value is 0.52. However, the overall membership value for Attack 7 is 0.76 which indicates that Attack 7 is much stronger compared to Attacks 4 and 9.

The above scenarios indicate that the system would assess the overall impact of the attack as measured by the fuzzy logic based Werners function given in Equation (7). This overall impact is based on the intensity of individual attacks for data given in Table II.

TABLE I. MAPPING OF KDD99 ATTACK TYPES TO STRIDE MODEL.

Attack Name in KDD99	Attack Category	STRIDE Attack Type
Mscan	Probe	Spoofing
Nmap	Probe	Spoofing
Portsweep	Probe	Spoofing
Saint	Probe	Spoofing
Satan	Probe	Spoofing
ftp_write	r2l	Tampering
guess_passwd	r2l	Tampering
Httptunnel	r2l	Tampering
Imap	r2l	Tampering
Warezclient	r2l	Repudiation
Warezmaster	r2l	Repudiation
Worm	r2l	Repudiation
Xlock	r2l	Repudiation
Xsnoop	r2l	Repudiation
Multihop	r2l	Information Disclosure
Named	r2l	Information Disclosure
Phf	r2l	Information Disclosure
Sendmail	r2l	Information Disclosure
Snmpgetattack	r2l	Information Disclosure
Snmpguess	r2l	Information Disclosure
Spy	r2l	Information Disclosure
apache2	Dos	Denial of Service
Back	Dos	Denial of Service
Land	Dos	Denial of Service
Mailbomb	Dos	Denial of Service
Neptune	Dos	Denial of Service
Processtable	Dos	Denial of Service
Udpstorm	Dos	Denial of Service
buffer_overflow	u2r	Elevation of Privileges
Loadmodule	u2r	Elevation of Privileges
Perl	u2r	Elevation of Privileges
Ps	u2r	Elevation of Privileges
Rootkit	u2r	Elevation of Privileges
Sqlattack	u2r	Elevation of Privileges
Xterm	u2r	Elevation of Privileges

CONCLUSION

This work proposed threat modeling by applying fuzzy logic based approach to the STRIDE threat model. The crisp numbers signifying the number of attacks on network systems were given as input. These numbers of attacks were fuzzified and then evaluated using the Werners operator. The result then led us to decide the level of attack. Preliminary empirical analysis indicates that the proposed approach satisfactorily addresses the issues of measuring impact of several simultaneous attacks.

Acknowledgment

The author thanks the Deanship of Scientific Research at University of Bahrain for supporting this work through Project # 24/2015. Thanks are also due to Mr. Faiz Iqbal for his assistance.

TABLE II. ATTACKS TYPES AND FREQUENCIES OF ATTACKS FOR 20 DIFFERENT ATTACKS.

Attack	S (0 - 10)	T (0 - 10)	R (0 - 5)	I (0 - 5)	D (0 - 10)	E (0 - 5)	Total number of Attacks
Attack 1	7	0	0	0	0	0	7
Attack 2	0	4	3	0	0	2	9
Attack 3	3	3	3	3	2	2	16
Attack 4	5	7	0	3	1	1	17
Attack 5	0	0	6	0	10	4	20
Attack 6	9	9	0	0	9	0	27
Attack 7	2	2	5	3	4	1	17
Attack 8	8	0	0	5	10	3	26
Attack 9	4	6	0	0	7	0	17
Attack 10	0	0	0	0	0	2	2

TABLE III. MEMBERSHIP VALUES OF ATTACKS AND OVERALL LEVEL. H = HIGH, M= MODERATE, L = LOW.

Attacks	μ_S	μ_T	μ_R	μ_T	μ_D	μ_E	f(x)	Level
Attack 1	0.70	0.00	0.00	0.00	0.00	0.00	0.44	Moderate
Attack 2	0.00	0.40	0.60	0.00	0.00	0.40	0.44	Moderate
Attack 3	0.30	0.30	0.60	0.60	0.20	0.40	0.53	High
Attack 4	0.50	0.70	0.00	0.60	0.10	0.20	0.55	High
Attack 5	0.00	0.00	1.20	0.00	1.00	0.80	0.90	High
Attack 6	0.90	0.90	0.00	0.00	0.90	0.00	0.71	High
Attack 7	0.20	0.20	1.00	0.60	0.40	0.20	0.76	High
Attack 8	0.80	0.00	0.00	1.00	1.00	0.60	0.83	High
Attack 9	0.40	0.60	0.00	0.00	0.70	0.00	0.52	High
Attack 10	0.00	0.00	0.00	0.00	0.00	0.40	0.25	Low

REFERENCES

[1] The STRIDE Threat Model, http://msdn.microsoft.com/enus/library/ee823878%28v=cs.20%29.aspx, 2002

[2] M. Curtin, Introduction to Network Security, Kent Information Services, Inc., March 1997.

[3] A. S. Sodiya, S. A. Onashoga and B. A. Oladunjoye, Threat Modeling using Fuzzy Logic Paradigm, Volume 4, 2007.

[4] A. Shostack, S. Lambert, S. Hernan, Uncover Security Design Flaws using STRIDE, MSDN magazine, November 2006.

[5] S. S. Godil, M. S. Shamim, Fuzzy logic: A "simple" solution for complexities in neurosciences?, http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3050069/

[6] C. Wijayayunga, Internet and Network Security Fundamentals, pg. 10-20, 1990

[7] W. Stalling, L. Brown, Computer Security: Principles and Practice, 2nd edition, Pearson Education, 2008.

[8] M. A. Anton, J. M. Barnes, STRIDE-based Security model, Institute of software research, January 2010.

[9] L. A. Zadeh. Fuzzy Sets. Information Control, 8:338–353, 1965.

[10] B. Floyd, The Changing Face of Network Security Threats, IEEE, SCTE, May 2006.

[11] J. E. Canavan, Fundamentals of Network Security, Artech House telecommunications library, 1999.

[12] Adeyinka, O., Internet Attack Methods and Internet Security Technology, Modeling and Simulation, 2008. AICMS 08. Second Asia International Conference on, pg. 77-72, Nov 2005.

[13] T. Ohta, T. and T. Chikaraishi, Network Security Model, http://www.sans.org/reading-room/whitepapers/modeling/network-security-model-32843, Accessed Jan. 2016.

[14] B. Werners. An interactive fuzzy programming system. *Fuzzy Sets and Systems*, 23:131–147, 1987.

[15] B. Werners. Aggregation models in mathematical programming. *G. Mittra, H. Greenberg, F. Lootsma, M. Rijckaert, and H. Zimmerman (Eds.) Mathematical Models for Decision Support, Springer*, 48:295305,1988.

[16] M. K. Siddiqui and S. Naahid, Analysis of KDD CUP 99 Dataset using Clustering based Data Mining, International Journal of Database Theory and Application Vol.6, No.5 (2013), pp.23-34

[17] D. Nyambo, Z. Yonah, and C. Tarimo. An Approach for Systematically Analyzing and Specifying Security Requirements for the Converged Web-Mobile Applications. International Journal of Computing and Digital Systems, Vol. 3, No. 3, pp. 207-217, Sept. 2014.

[18] E. Cambiaso, G. Papaleo, G. Chiola , and M. Aiello. A Network Traffic Representation Model for Detecting Application Layer Attacks. Vol. 5, No.1, pp. 32-42, Jan. 2016

Salman A. Khan received Ph.D. in computer science from University of Pretoria, South Africa in 2009. He is currently an Assistant Professor of Computer Engineering at University of Bahrain. He has over 40 publications in reputed journals and conferences. His research areas are evolutionary computation, fuzzy logic optimization, network design and optimization, and network security.