Internal Intrusion Detection System and Protection using Data Mining and Forensic Methodology

Rawat Vishal Shivaji
Someshwar Tal. Phaltan Dist. Satara India

Abstract— Currently, most computer systems use somebody IDs and passwords as the login patterns to authenticate users. Nevertheless, many group percentage their login patterns with coworkers and postulation these coworkers to assist co-tasks, thereby making the activity as one of the weakest points of machine security. Insider attackers, the validated users of a system who aggress the scheme internally, are hardened to sight since most intrusion detection systems and firewalls identify and isolate despiteful behaviors launched from the external humans of the group exclusive. In improver, whatsoever studies claimed that analyzing group calls (SCs) generated by commands can name these commands, with which to accurately discover attacks, and start patterns are the features of an crime. Thus, in this material, a guard scheme, titled the Inside Intrusion Find and Covering Method (IIDPS), is planned to notice insider attacks at SC structure by using data defence and forensic techniques. The IIDPS creates users' individualized profiles to reserve cartroad of users' usance habits as their forensic features and determines whether a sensible login someone is the reason capitalist or not by examination his/her flow computer employment behaviors with the patterns collected in the ground holder's personalised salience. The experimental results corroborate that the IIDPS's somebody determination quality is 94.29%, whereas the salutation quantify is little than 0.45 s, implying that it can preclude a stormproof method from insider attacks effectively and efficiently.

Key words: Data Mining, Insider Attack, Intrusion Detection and Protection, System Call (SC), Users' Behaviors

I. INTRODUCTION

In the other decades, computer systems possess been widely working to wage users with easier and solon convenient lives. Nonetheless, when people work puissant capabilities and processing nation of computer systems, guard has been one of the real problems in the computer environment since attackers real unremarkably try to perforate machine systems and move maliciously, e.g., concealing dangerous aggregation of a organisation, making the systems out of process or equal destroying the systems. Mostly, among all well-known attacks such as pharming crime, dispensed denial-of-service (DDoS), eavesdropping assault, and spear-phishing criticize [1], [2], insider operation is one of the most troublesome ones to be sensed because firewalls and intrusion detecting systems (IDSs) ordinarily back against outdoors attacks. To authenticate users, currently, most systems review somebody ID and password as a login route. However, attackers may position Trojans to lift victims' login patterns or supply a capacious leaf of trials with the assistance of a lexicon to chisel users' passwords.

When successful, they may then log in to the system, accession users' confidential files, or add or defeat method settings. Luckily, most new host-based guarantee systems [3] and network-based IDSs [4], [5] can learn a notable intrusion in a real-time manner. Withal, it is real ambitious to key who the assailant is because aggress packets are oftentimes issued with forged IPs or attackers may succeed a group with reasoned login patterns. Tho' OS-level system calls (SCs) are often author attending in sleuthing attackers and identifying users [6], processing a mammoth volume of SCs, defense spiteful behaviors from them, and identifying accomplishable attackers for an intrusion are relieve study challenges. Thence, in this production, we request a safeguard method, titled Intimate Intrusion Reception and Imposition Group (IIDPS), which detects despiteful behaviors launched toward a scheme at SC storey. The IIDPS uses collection production and forensic profiling techniques to mine scheme song patterns (SC-patterns) settled as the long scheme phone successiveness (SC-sequence) that has repeatedly appeared individual times in a user's log enter for the mortal. The user's forensic features, distinct as an SC-pattern of attendance in a user's submitted SC-sequences but rarely beingness utilised by additional users, are retrieved from the user's machine usage chronicle. The contributions of this stuff are: 1) denote a user's forensic features by analyzing the like SCs to deepen the accuracy of move find; 2) competent to opening the IIDPS to a antiparallel scheme to added shorten its catching greeting quantify; and 3) effectively disobey insider act.

II. REVIEW OF LITERATURE

Computer forensics science, which views machine systems as transgression scenes, aims to refer, area, ameliorate, study, and present facts and opinions on substance collected for a assets circumstance [7]. It analyzes what attackers fuck through such as spreading computer viruses, malwares, and despiteful codes and conducting DDoS attacks [8]. Most intrusion discovery techniques nidus on how to exploit vindictive system behaviors [9], [10] and win the characteristics of crime packets, i.e., onslaught patterns, based on the histories transcribed in log files [11], [12]. Qadeer et al. [13] old self-developed boat sniffer to amass mesh packets with which to tell meshing attacks with the better of mesh states and packet spacing. O' Shaughnessy and Poet [14] acquired meshing intrusion and operation patterns from system log files. These files comprise traces of computer utilisation. It agency that, from synthetically generated log files, these traces or patterns of utilisation can be statesman accurately reproduced. Wu and Banzhaf [15] overviewed search movement of applying methods of computational tidings, including painted neuronal networks, fuzzy systems, evolutionary computing, colored transmitter systems, and stream information, to discover despiteful behaviors. The authors systematically summarized and compared incompatible intrusion discovery methods, thusly allowing us to understandably see those existing investigate challenges.

These said techniques and applications truly further to fabric safeguard. Notwithstanding, they cannot easily authenticate remote-login users and notice circumstantial types of intrusions, e.g., when an unlicenced user logs in to a

method with a sound person ID and countersign. In our early learning [16], a precaution group, which collects forensic features for users at statement rank kinda than at SC steady, by invoking information defense and forensic techniques, was mature. Moreover, if attackers use galore sessions to provision attacks, e.g., multistage attacks, or move DDoS attacks, then it is not casual for that grouping to name criticize patterns. Hu et al. [17] presented an alert lightweight IDS that utilizes a forensic model to profile mortal behaviors and a data defense technique to fuddle out noncompetitive attacks. The authors claimed that the group could detect intrusions effectively and expeditiously in genuine clip. Withal, they did not reference the SC filtrate. Giffin et al. [18] provided another representative of integrating machine forensics with a knowledge-based method. The group adopts a predepunished leader, which, allowing SC-sequences to be normally executed, is exploited by a sleuthing method to circumscribe show.

Subscription to secure the section of the battlemented grouping. This is accommodative in sleuthing applications that yield a serial of malicious SCs and identifying commencement sequences having been composed in noesis bases. When an undiscovered formulation is presented, the method oft finds the assail successiveness in 2 s as its procedure return. Fiore et al. [19] explored the effectivity of a catching movement based on organization learning using the Discriminative Limited Boltzmann Machine to feature the expressive cognition of productive models with swell classification accuracy capabilities to conclude object of its noesis from uncomplete preparation assemblage so that the scheme anomaly spotting grouping can engage an passable makings of shelter from both external and intrinsical menaces. Faisal et al. [20] analyzed the opening of using data current defense to heighten the protection of innovative metering infrastructure finished an IDS. The advanced metering infrastructure, which is one of the most pivotal components of intelligent separate.

III. EXISTING SYSTEM

In existing group, a supporter is proposed for much an crime supported on meshwork traffic flow. Particularised fabric topology-based patterns are definite to modelling inborn meshwork interchange feed, and to ease secernment between rightful traffic packets and anomalous snipe interchange packets. A new motion for postmortal intrusion perception, which factors out continual doings, thusly move up the treat of locating the enforcement of an exploit, if any. Work to our intrusion detection performance is a classifier, which separates supernormal action from pattern one. This classifier is stacked upon a method that combines a unseeable Markov display with k -means. Packet sniffer is not vindicatory a hackers agency. It can be victimized for meshwork reciprocation monitoring, reciprocation psychotherapy, troubleshooting and other useful purposes. When computers interact over networks, they unremarkably retributive focus to the reciprocation specifically for them. The separate is that they cannot easily authenticate remote-login users and discover fact types of intrusions.

A. *Drawback of Existing System*

1) *Problem Statement*

The proposed scheme give a warranty grouping, named Intrinsical Intrusion Catching and Indorsement Grouping (IIDPS), which detects leering behaviors launched toward a group at SC layer. The IIDPS uses information defense and forensic profiling techniques to mine scheme call patterns (SC patterns) formed as the longest grouping option order that has repeatedly materialise various present in a users log file for the mortal. The users forensic features, characterized as an SC imitate often attending in a users submitted SC ordering but rarely being utilised by another users ,are retrieved from the users computer utilization account. The scheme need to acquisition the SCs generated and the SC-patterns produced by these commands so that the IIDPS can notice those spiteful behaviors issued by them and then forestall the secure system from state attacked. The proposed database intrusion espial method consists of log excavation mechanism and an intrusion spotting performance. In this we are using agent idea for spotting of intrusion. Agent is regalia list with extended properties which follows projectile and handgun plus of assemblage at run minute. So it reduces the computations. In this we are production log file for alikeness resolution to observe intrusion. Initially, system copies the listing from log record into temporary record as no one can accomplish operations on log file flat. Then with model database the comparability is carried out.

IV. PROPOSE WORK

A. *System Architecture*

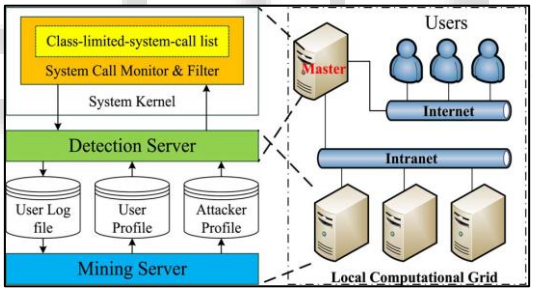

Fig. 1: IIDPS System Architecture

1) *System Framework*

The IIDPS, as shown in Fig. 1, consists of an SC monitor and filter, an excavation server, a spying server, a localised computational grid, and tierce repositories, including somebody log files, soul profiles, and a wrongdoer salience. The SC monitor and filtrate, as a loadable module embedded in the sum of the scheme state considered, collects those SCs submitted to the inwardness and stores these SCs in the dissever of uid, pid, SC in the secure grouping where uid, pid, and SC respectively embody the individual ID, the transform ID, and the SC c submitted by the underlying somebody, i.e., $c \in SCs$. It also stores the soul inputs in the user's log file, which is a enter safekeeping the SCs submitted by the mortal multitude their submitted succession. The mining computer analyzes the log information with accumulation mining techniques to set the user's machine usage habits as his/her action patterns, which are then transcribed in the user's mortal strikingness. The spotting computer ompares users' behavior patterns with those SC-patterns collected in the aggressor saliency, called criticise patterns, and those in user profiles to respectively observe malicious behaviors and key who the

wrongdoer is in proper moment. When an intrusion is observed, the espial computer notifies the SC reminder and filtrate to discriminate the mortal from the bastioned group. The role is to forestall him/her from continuously offensive the system.

2) SC Monitoring and filter

An SC in fact is an program between a soul program and services provided by the marrow. Mostly, a immense amount of SCs are generated during the subscription of a job, i.e., a task or touch. For representative, when a individual changes his/her secret by submitting a "passwd" withdraw say to a Linux operating group, up to 2916 SCs present be generated, including arise(), uncommunicative(), register(), pen(), etc. Thus, it is intemperate for a system to monitor all SCs at the said quantify, especially when numerous users are spurting their programs. As a termination, we essential to filter out any commonly victimized harmless SCs. To encounter out what SCs are characteristic ones generated by a cover lie, the statistic imitate of period frequency-inverse credit frequency (TF-IDF) is old to study the importance of intercepted SCs composed in a person log file. In the aggregation deed domain, the relation between a point and a document is related to that between an SC ti and the mastery, e.g., j, which generates ti. The point rate (TF) employed to amount the weight of the oftenness of an SC produced by j is formed as

Command	No of SC	SC Genetated
chmod	94	Close(3),read(20).open(30), execver(1), access(10), brk(10), unmask(10), munmap(4), mprotect(3), mmap2(3)
kill	47	Close(2), read(10).open(10), execver(1), access(10), brk(2), unmask(2), munmap(4), mprotect(3), mmap2(3)
date	58	Close(3), read(10).open(10), execver(1), access(10), brk(2), unmask(2), munmap(4), mprotect(3), mmap2(13)
rm	74	Close(3), read(10).open(10), execver(1), access(10), brk(10), unmask(20), munmap(4), mprotect(3), mmap2(3)

Table 1: SCS and their Generation Frequencies during the Execution of four Specific Commands

3) Mining Server

As shown in Fig. 1, a defense server extracts SC-equence generated by a soul u from u's log file, counts the times that a particularized SC-pattern appears in the line, and stores the prove in SC-pattern, appearance counts information in u's use enter. After this, SC-patterns' similarity weights are calculated to separate out those SC-patterns commonly used by all or most users. Then, the yield prove is compared with all remaining users' misuse files in the underlying group to encourage refer u's specific Scpatterns. Finally, the similarity unit is computed to make u's someone saliency.

4) Advantages of Propose System

- It is more secure.
- Usgin Data Mining Serve to store user SC Patter.
- Prevants from DOS attach.

B. Propose Algorithm

1) Algorithm No 1

The Algorithm for generating a user habit file

- Input: us log file where u is a user of the underlying system
- Output: us habit file

1) G = | log file | - | Sliding window |;
2) for (i=0; i = G-1; i++) {
3) for (j=i+1; j=G; j++) {
4) for (each of (|Sliding Window| - k+1) k-grams in current L-window){
5) for(each of(|Sliding Window| -´k+1) ´k-grams in current C-window){
6) Compare the k-grams and ´k-grams with the longest common subsequence algorithm;
7) if(the identified SC-pattern already exists in the habits file)
8) Increase the count of the SC-pattern by one ;
9) else
10) Insert the SC-pattern into the habit file with count=1;}}}}

2) Algorithm No 2

Detecting an internal intruder or an attacker

- Input: uuuser ´us current input SCs, i.e., NSCu,(each time only one SC is input), and all users user profile
- Output: u is suspected as an internal intruder or a known attacker

1) NCSu=Ø;
2) while (receiving ´us input SC,denoted by h){
3) NCSu = NCS ?{h }
4) if(|NCSu)>|Sliding Window|{
5) L-window = Right(NCSu | Sliding window |);
6) for(j=|NCSu | - | Sliding window |; j>0;j–){
7) C-window =| (NCSu,j, | Sliding window |);/*Mid (x,y,z)retrives a sliding window of size z begining at the position of y from x */
8) Compare k-grams and ´k-grams by using the comparision logic employed in algorithm 1 to generate NHFu;}
9) for (each user g, 1 = g = N)
10) Calculate the similarity score Sim(u,j) between NCSu and ´gs user profile by invoking Equation
11) if((|NCSu | mod paragraph size)==0){ /* paragraph size =30, meaning we judge whether u is an attacker or the account holder for every 30 input SCs*/
12) Sort similarity scores for all users;
13) if((the decisive rate of ´u s user profile ¡ threshold1)or (the decisive rate of attacker profile ¿ threshold2)){/* threshold1 is the predefined lower bound of average decisive rate of user ´us user profile, while threshold2 is the predefined upper bound of average decisive rate of attacker profile */
14) Alert system manager that u is a suspected attacker, rather than u himself/herself; }}}}

C. Mathematical Module

Which is the number of sliding windows that can be identified in the given SC-sequence. Then, a user profile is generated by invoking $|m*(m-1)/2|$ times of the L-window,C-window pairwise comparison, and each L-window,C-window pairwise comparison has.

$$\sum_{K=2}^{|\text{Sliding Window}|} (|\text{Sliding Window}|-K+1) * \sum_{K'=2}^{|\text{Sliding Window}|} (|\text{Sliding Window}|-K'+1)$$

This means that the time complexity of k-gram, k -gram comparison is O(n6). Of course, if we consider the time complexity on l, it will be O(l 2). Fig. 5 gives an example of k-gram, k -gram comparison. The solid-line rectangles list two compared SC-sequences. A shaded area is a C-window. The dash-line rectangle contains an SC-sequence, i.e., a k-gram, extracted from an L-window where k = 10. In the upper rectangle (i.e., marked with C-window 1), SCs that match those in the k -gram where k = 10 include brk, fstat64, and mprotect (omitting () of an SC for simplicity). The remaining SCs, including close, open, read, access, open, mmap2, and write, are noises and thus ignored. When k = k = 10, the longest common subsequence between the k-gram and the k -gram in the lower rectangle (marked with C-window 2) includes execve, access, open, open, and brk.

Stores the SCs in the u's log file. After this, the server tries to identify whether u is the underlying account holder or not by calculating the similarity score between the newly generated SCs, denoted by NSCu, in the u's current inputs (in u's log file) and the usage habits, i.e., forensic signatures (also behavior patterns), stored in u's user profile to verify u. The Okapi model [24], which is utilized to calculate the similarity score between user j's user profile UHj and an unknown user u's current input SC-sequence, denoted by Sim(u, j), is defined as

$$\text{Sim}(u, j) = \sum_{i=1}^{p} \text{Fiu} \cdot \text{Wij}$$

In which p is the number of SC-patterns appearing in both NCSu and UHj, Fiu is the appearance count of SC-pattern i collected in NCSu, and Wij produced by invoking (7) is the similarity weight of i in UHj. The higher the Sim(u, j), the higher the probability, with which u is the person j who submitted NCSu.

V. IMPLEMENTATION STATUS

Here are some modules required in implementing the IIDP in our project.

A. System User

In this module we create system user account and setup account with same disk space on system as per user need.

B. User Habit File

In this module we monitor user every system call and store into user habit on file, we call it user log file. In user log file write user SC data on {user id, process id, SC} formate.

C. Attack Detection

In this module we implement Algorithm No1 and Algorithm No 2. For detect internal attack.

Implementation is as follow,

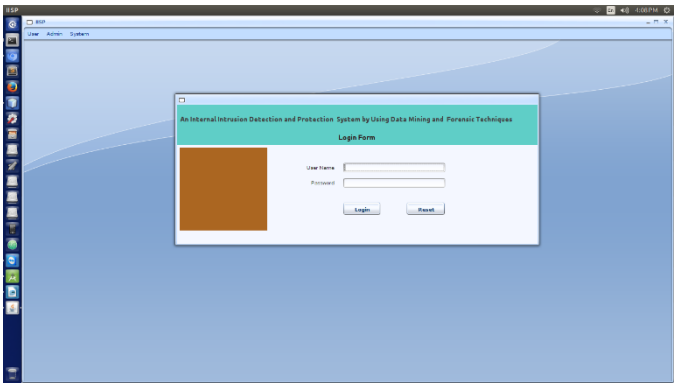

Fig. 2: User Login.

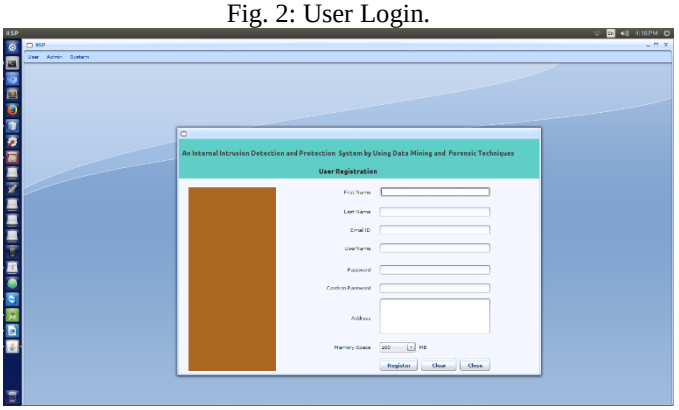

Fig. 3: User Registration.

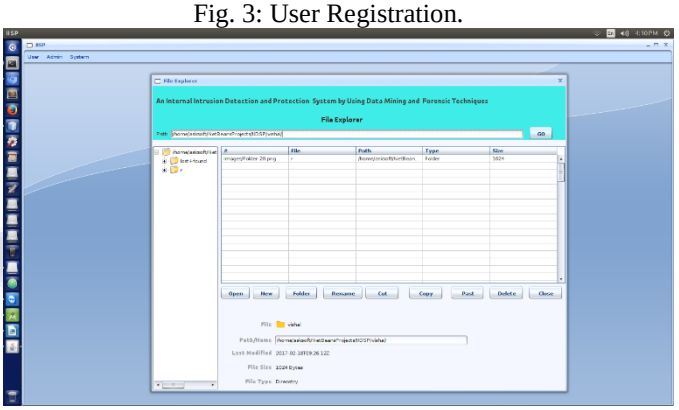

Fig. 4: Implementation

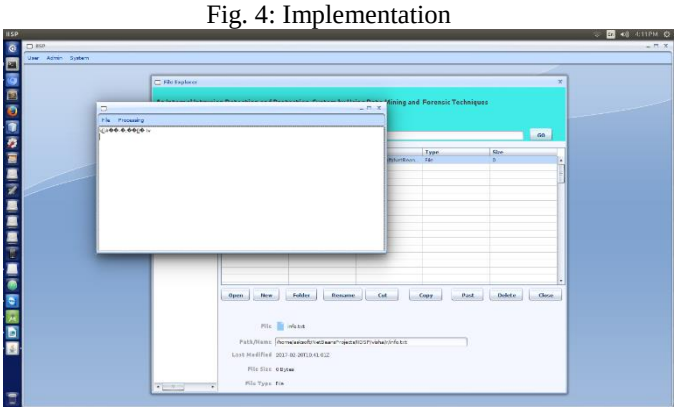

Fig. 5: Implementation

VI. EXPERIMENTAL SETUP

The system is built using Java, (version J2SDK 1.7 / 1.8), SDK tool MySQL database on Linux Ubuntu platform. The experiments have been performed on the machine with the following specifications: Intel Core 2 dual processor with 2.5 GHz CPU, 2 GB RAM, 180 GB Hard disk and running Ubuntu 16.04 LTS x64.

VII. RESULT TABLE AND OUTCOME SUCCESS WORK

To verify the feasibility and truth of the IIDPS, leash experiments were performed. The front definite the deciding assess boundary between the user saliency grooved for u and apiece of opposite users' person profiles. The support studied the accuracy for the online spying computer when NCSu was submitted by u. The third compared the IIDPS with several state-of-the-art hostbased IDSs (HIDSs).

Account	Training Data	Habit File	User Profile
Vishal	9531	122,805	73,688
Kishor	10,203	203,120	80,532
Kiran	8,255	98,253	50,553
Santosh	6,648	70,468	89,521

Table 2: User Profiles Generated by the Mining Server in Parallel

For shrewd decisive valuate time evaluating the user's examine collection where the paragraph filler is 30 SCs, "Nowadays of existence an record holder" is the cypher nowadays of its multiple worth that conclusive value is larger than the predefined limen, and "Nowadays of existence an attacker" is the moderate present of its multiple worth that the determining rates are smaller than predefined verge, i.e., the times that the detecting server alerts the method trainer that the current person is an offender

VIII. CONCLUSION

We have proposed an approach that employs data mining and forensic techniques to identify the representative SC-patterns for a user. The time that a habitual SCpattern appears in the users log file is counted, the most commonly used SC-patterns are filtered out, and then a users profile is established. By identifying a users SC-patterns as his/her computer usage habits from the users current input SCs, the IIDPS resists suspected attackers.

REFERENCES

[1] S. Gajek, A. Sadeghi, C. Stuble, and M. Winandy, "Compartmented security for browsers—Or how to thwart a phisher with trusted computing," in Proc. IEEE Int. Conf. Avail., Rel. Security, Vienna, Austria, Apr. 2007, pp. 120–127.

[2] C. Yue and H. Wang, "BogusBiter: A transparent protection against phishing attacks," ACM Trans. Int. Technol., vol. 10, no. 2, pp. 1–31, May 2010.

[3] Q. Chen, S. Abdelwahed, and A. Erradi, "A model-based approach to self-protection in computing system," in Proc. ACM Cloud Autonomic Comput. Conf., Miami, FL, USA, 2013, pp. 1–10.

[4] F. Y. Leu, M. C. Li, J. C. Lin, and C. T. Yang, "Detection workload in a dynamic grid-based intrusion detection environment," J. Parallel Distrib. Comput., vol. 68, no. 4, pp. 427–442, Apr. 2008.

[5] H. Lu, B. Zhao, X. Wang, and J. Su, "DiffSig: Resource differentiation based malware behavioral concise signature generation," Inf. Commun. Technol., vol. 7804, pp. 271–284, 2013.

[6] Z. Shan, X. Wang, T. Chiueh, and X. Meng, "Safe side effects commitment for OS-level virtualization," in Proc. ACM Int. Conf. Autonomic Comput., Karlsruhe, Germany, 2011, pp. 111–120.

[7] M. K. Rogers and K. Seigfried, "The future of computer forensics: A needs analysis survey," Comput. Security, vol. 23, no. 1, pp.12–16, Feb. 2004.

[8] J. Choi, C. Choi, B. Ko, D. Choi, and P. Kim, "Detecting web based DDoS attack using MapReduce operations in cloud computing environment," J. Internet Serv. Inf. Security, vol. 3, no. 3/4, pp. 28–37, Nov. 2013.

[9] Q. Wang, L. Vu, K. Nahrstedt, and H. Khurana, "MIS: Malicious nodes identification scheme in network-coding-based peer-to-peer streaming," in Proc. IEEE INFOCOM, San Diego, CA, USA, 2010, pp. 1–5.

[10] Z. A. Baig, "Pattern recognition for detecting distributed node exhaustion attacks in wireless sensor networks," Comput. Commun., vol. 34, no. 3, pp. 468–484, Mar. 2011.

[11] H. S. Kang and S. R. Kim, "A new logging-based IP traceback approach using data mining techniques," J. Internet Serv. Inf. Security, vol. 3, no. 3/4, pp. 72–80, Nov. 2013.

[12] K. A. Garcia, R. Monroy, L. A. Trejo, and C. Mex-Perera, "Analyzing log files for postmortem intrusion detection," IEEE Trans. Syst., Man, Cybern., Part C: Appl. Rev., vol. 42, no. 6, pp. 1690–1704, Nov. 2012.

[13] M. A. Qadeer, M. Zahid, A. Iqbal, and M. R. Siddiqui, "Network traffic analysis and intrusion detection using packet sniffer," in Proc. Int. Conf. Commun. Softw. Netw., Singapore, 2010, pp. 313–317.

[14] S. O'Shaughnessy and G. Gray, "Development and evaluation of a data set generator tool for generating synthetic log files containing computer attack signatures," Int. J. Ambient Comput. Intell., vol. 3, no. 2, pp. 64–76, Apr. 2011.

[15] S. X. Wu and W. Banzhaf, "The use of computational intelligence in intrusion detection systems: A review," Appl. Soft Comput., vol. 10, no. 1, pp. 1–35, Jan. 2010.

[16] F. Y. Leu, K. W. Hu, and F. C. Jiang "Intrusion detection and identification system using data mining and forensic techniques," Adv. Inf. Comput. Security, vol. 4752, pp. 137–152, 2007.

[17] Z. B. Hu, J. Su, and V. P. Shirochin "An intelligent lightweight intrusion detection system with forensics technique," in Proc. IEEE Workshop Intell. Data Acquisition Adv. Comput. Syst.: Technol. Appl., Dortmund, Germany, 2007, pp. 647–651.

[18] J. T. Giffin, S. Jha, and B. P. Miller, "Automated discovery of mimicry attacks," Recent Adv. Intrusion Detection, vol. 4219, pp. 41–60, Sep. 2006.

[19] U. Fiore, F. Palmieri, A. Castiglione, and A. D. Santis, "Network anomaly detection with the restricted Boltzmann machine," Neurocomputing, vol. 122, pp. 13–23, Dec. 2013.

[20] M. A. Faisal, Z. Aung, J. R. Williams, and A. Sanchez, "Data-streambased intrusion detection system for advanced metering infrastructure in smart grid: A feasibility study," IEEE Syst. J., vol. 9, no. 1, pp. 1–14, Jan. 2014.

[21] R. J. Roger and M. W. Geatz, Data Mining: A Tutorial-Based Primer. Reading, MA, USA: Addison-Wesley, 2002.

[22] S. J. Shyu and C. Y. Tsai, "Finding the longest common subsequence for multiple biological sequences by ant

colony optimization," Comput. & Oper. Res., vol. 36, no. 1, pp. 73–91, Jan. 2009.
[23] D. Zhu and J. Xiao, "R-tfidf, a Variety of tf-idf Term Weighting Strategy in Document Categorization," in Proc. Int. Conf. Semantics, Knowledge Grids, Beijing, China, Oct. 2011, pp. 83–90.
[24] S. E. Robertson, S. Walker, M. M. Beaulieu, M. Gatford, and A. Payne, "Okapi at TREC-4," in Proc. 4th text Retrieval Conf., 1996, pp. 73–96.
[25] S. Yu, K. Sood, and Y. Xiang, "An effective and feasible traceback scheme in mobile internet environment," IEEE Commun. Lett., vol. 18, no. 11, pp. 1911–1914, Nov. 2014.
[26] B. Sayed, I. Traore, I. Woungang, and M. S. Obaidat, "Biometric authentication using mouse gesture dynamics," IEEE Syst. J., vol. 7, no. 2, pp. 262–274, Jun. 2013.
[27] S. C. Arseni, E. C. Popovici, L. A. Stancu, O. G. Guta, and S. V. Halunga, "Securing an alerting subsystem for a keystroke-based user identification system," in Proc. Int. Conf. Commun., Bucharest, Romania, 2014, pp. 1–4.
[28] G. M. Amdahl, "Validity of the single processor approach to achieving large scale computing capabilities," in Proc. AFIPS Spring Joint Comput. Conf., New Brunswick, NJ, USA, 1967, pp. 1–4.

