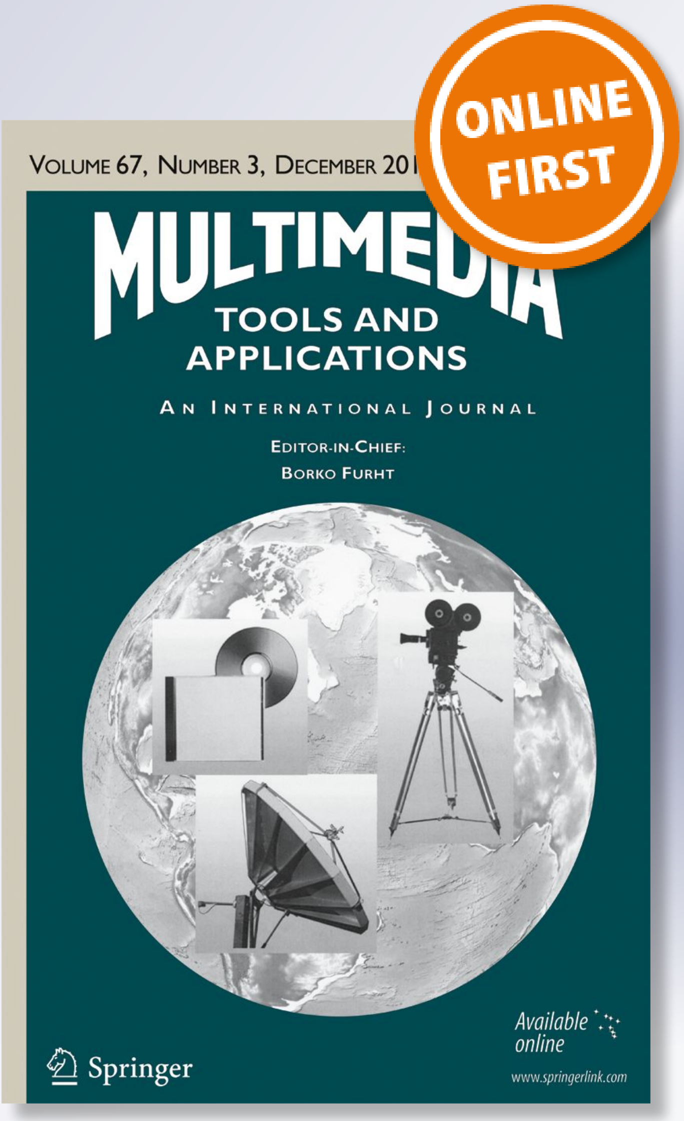
Context-aware multimodal recommendations of multimedia data in cyber situational awareness

Awny Alnusair, Chen Zhong, Majdi Rawashdeh, M. Shamim Hossain & Atif Alamri

Multimedia Tools and Applications
An International Journal

ISSN 1380-7501

Multimed Tools Appl
DOI 10.1007/s11042-017-4681-2



Springer

Your article is protected by copyright and all rights are held exclusively by Springer Science +Business Media New York. This e-offprint is for personal use only and shall not be self-archived in electronic repositories. If you wish to self-archive your article, please use the accepted manuscript version for posting on your own website. You may further deposit the accepted manuscript version in any repository, provided it is only made publicly available 12 months after official publication or later and provided acknowledgement is given to the original source of publication and a link is inserted to the published article on Springer's website. The link must be accompanied by the following text: "The final publication is available at link.springer.com”.

Springer

Author's personal copy

Multimed Tools Appl
DOI 10.1007/s11042-017-4681-2

Context-aware multimodal recommendations of multimedia data in cyber situational awareness

Awny Alnusair[1] · Chen Zhong[1] · Majdi Rawashdeh[2] · M. Shamim Hossain[3,4] · Atif Alamri[3,4]

Received: 29 October 2016 / Revised: 28 March 2017 / Accepted: 3 April 2017
© Springer Science+Business Media New York 2017

Abstract The current proliferation of large amounts of multimedia data creates an unprecedented challenge for security analysts in the context of Cyber Situational Awareness. Due to this phenomenal growth of multimedia data, security analysts have to invest enormous time and efforts in filtering and correlating multimedia data in order to make informed decisions about identifying and mitigating threats and vulnerabilities. In particular, analysts have to analyze and interpret diverse multimedia network data with varying contexts in order to find the true evidence of cyber attacks. Considering the multimedia nature of cyber security data, we propose a cloud-assisted recommendation system that can identify and retrieve multimedia data of interest based on contextual information and security analysts' personal preferences. This recommendation system benefits security analysts by establishing a bridge

✉ M. Shamim Hossain
mshossain@ksu.edu.sa

Awny Alnusair
alnusair@iuk.edu

Chen Zhong
chzhong@iuk.edu

Majdi Rawashdeh
m.rawashdeh@psut.edu.jo

Atif Alamri
atif@ksu.edu.sa

[1] Department of Informatics and Computer Science, Indiana University, Kokomo, IN 46904, USA

[2] Department of Management Information Systems, Princess Sumaya University for Technology, Amman, Jordan

[3] Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia

[4] Research Chair of Pervasive and Mobile Computing, King Saud University, Riyadh 11543, Saudi Arabia

Published online: 18 April 2017

Author's personal copy

between their personal preferences, the contextual information of their analytical process, and the various types of modality of multimedia data. Evaluation of the proposed system shows evidence that our multimedia recommendation mechanisms promotes cyber threat understanding and risk assessment.

Keywords Cyber situational awareness · Multimedia recommendation · Cyber security · Context awareness · Cloud computing

1 Introduction

The already existing overwhelming amounts of multimedia data that comes in various forms of modality (i.e., textual documents, video, audio, graphics, etc.) is continuing to grow on a daily basis [18]. Even though much of cyber security data can be found in textual documents (text modality), often times it can be embedded in other forms of modality such as audio, video and visual modalities as well. This multimedia data comes from diversified sources, including social media, multimedia databases, mobile and cloud services, and most importantly local and remote networks. Understandably, this phenomenon makes the process of identifying and recommending suitable multimedia contents an increasingly challenging task, especially for the purposes of aiding decision making in Cyber Situational Awareness.

Cyber Situational Awareness (aka. Cyber SA or CSA) attempts to employ systematic measures to collecting and analyzing data from various sources in order to provide security analysts with precise information for decision making about potential security threats. Many government agencies, corporations in the private sector, and the military have been investing money and resources to establish Security Operations Centers (SOCs) that can deal with the increasing levels of sophisticated cyber attacks. Such SOCs employ both cyber defense technologies and human security analysts. Generally speaking, cyber defense tools and technologies utilize various automated security measures in order to continuously monitor the generated network multimedia data that can come from sources such as packet dumps, firewall logs, vulnerability reports, and IDS/IPS alerts. Proper analysis of such network data can facilitate decision making and allow analysts to gain security awareness for more informed decision making and network remediation.

Network monitoring data is being collected at a rapid pace and from multiple network sensors. Most of this stream of data is well-formed but may have different formats across various sources as shown Fig. 1. Due to the massive and large volume of generated data, cyber analytics is an extremely challenging task for analysts. As such, achieving real-time situational awareness for cyber security threats requires effective mechanisms that identify and recommend suitable multimedia content for analysts to facilitate decision making during the process of preventing and mitigating harmful security accidents. Effective means to achieve this goal need to guide cyber analysts throughout the process of finding the “true threat signals” that require more attention from the existing massive amounts of multimedia data.

In order to support the retrieval and fusion of relevant multimedia data from various sources in cyber security awareness, we propose a multi-modal recommendation system that bridges the gap between the analyst’s context and the available multimedia recommendation options. Oftentimes, analysts may be interested in locating data of interest based on their current context of analysis (i.e., focus of attention) and their personal preferences and reasoning style. Therefore, our system personalizes the multimedia recommendations based on proper selection of contextual dimensions. In order to achieve this, our system attempts to understand the current state of the analyst by collecting and analyzing different

Author's personal copy

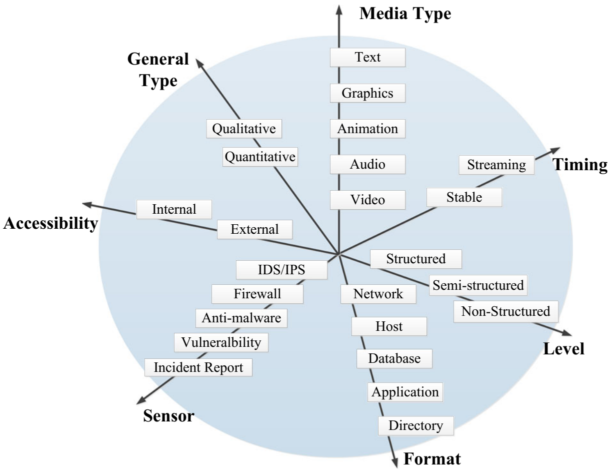


Fig. 1 Various data sources in cyber security awareness

physiological parameters that represent the typical interaction between the analyst and Cyber SA data. The system also applies cognitive task analysis methods that capture the analysts' mental model and understand his/her cognitive activities while performing the typical daily analysis tasks.

To this end, we have designed and implemented a context-aware recommendation system that simulates the complicated analytical process of cyber analysts. This is done by automating the process of inspecting multimedia network data for the purpose of revealing associations, patterns, and trends of cyber attacks. The system consists of several components, but most importantly it features a recommendation engine with reasoning capabilities that allows it to identify, rank, and personalize its recommendations based on the currently available contextual information. Furthermore, the system is flexible and scalable through incorporating Cloud Computing (CC) services in order to enhance the process of storing, managing, and processing the massive amounts of CSA data sets.

The work presented in this article contributes to establishing a bridge between Cyber SA and multimedia recommendation by providing a multi-modal recommender system that is capable of filtering various facets of multimedia contents in order to identify possible security threats for cyber analysts review. Additionally, there are several other contributions of this work. Firstly, in order to achieve timely and accurate assessment of threats and vulnerabilities in Cyber SA, the system features novel methods for capturing the fine-grained traces of the cognitive processes of cyber analysts. Secondly, the proposed system utilizes context-adaptive techniques to collect and incorporate contextual information in the recommendation process. Thirdly, in order to leverage the recommendation process, we developed a model that incorporates the detected context, the dimensions of Cyber SA data sources, and the historical traces of analysts' previous analytical knowledge. This model is backed by an algorithm that performs the matching and the ranking of items based on detecting the relationships among cyber analysts, contexts, and the multimedia items . Finally, recognizing the fact that cyber analysts need to swiftly respond to cyber threats, the proposed system is designed with principles of user-centered design techniques in mind. In particular, the system provides seamless interaction with analysts by automating the process of collecting and analyzing the information needed to simulate the analysts' analytical processes.

Author's personal copy

The rest of the paper is organized as follows: In the following section, we provide some background information about the essence of the problem at hand. We also, provide a detailed discussion about the current state-of-the-art in both Cyber SA and multimedia recommendations. In Section 3, we discuss the design and functionality of the various components that makeup the architecture of the proposed recommendation system. We further discuss and formalize the recommendation model and its experimental evaluation in Sections 4 and 5, respectively.

2 Background and literature review

There has been quite a significant body of research related to cyber situational awareness and multimedia recommendation systems, much of this work has been implemented into useful tools. However, we have not found a single context-aware approach that utilizes the full potential of Multimodal Information Retrieval (MMIR) search by incorporating the various facets of multimedia data when recommending credible threats for the security analyst's review . Therefore, we discuss these efforts separately.

2.1 Mutlimedia recommendation

Researchers have proposed many multimedia recommendation techniques, each of which tackle the recommendation problem from different perspectives. In this article, we focus the discussion on the most closely related recommendation approaches that do recommend personalized multimedia items when queried.

Today's recent advancements in technology that focuses on the interactions between multimedia users and the available variety of recommendation systems is getting a great deal of attention from both industry and academia. The goal is to enable a better user experience when searching for multimedia contents while handling of the tradeoff between multimedia security and ease of use [28]. In order to estimate the suitability of the recommended multimedia content to the user's current context is dependent upon the accurate selection of contextual dimensions during the recommendation process. In particular, capturing the user's state and the contextual information about the user's environment yields a more accurate and personalized recommendation of multimedia items.

Context-based recommendation of multimedia contents aims at recommending items that have not been recommended to the current user, but might have been recommended to contextually similar users based on similarity measures of their behaviors [11]. Other approaches utilizes context in multimedia adaptation to adapt the recommended items to specific choices by the user [19]. Dynamic user context was utilized adaptively for recommending ambient media services in smart home monitoring environments [10]. This work addresses the dynamic nature of media services and the dynamic nature of user interaction with the environment. It further discusses the challenges of securing network data in transit [12].

Other context-aware approaches tackle the recommendation problem from different perspectives and target different environments, including u-healthcare services [15], intelligent online shopping [2], and Ambient Intelligence (AmI) [1]. Closely related to our recommendation systems is the RecAm framework [1], which is a multi-modal recommendation framework that utilizes context-adaptive measures to recommend items in smart home environments using AmI adaptive user interfaces. These interfaces enhance context-awareness by utilizing sensors to gather environmental and physiological readings in real-time and

Author's personal copy

by incorporating additional social network information, multimedia data, and collaborative ratings to personalize recommendations.

Other context-aware recommendation approaches utilize social tagging services that organize and share social media content through collaborative tagging services (folksonomies). These approaches utilize various mechanisms to personalize recommendations and enhance the ranking of the recommended items. Such mechanisms apply graph-based algorithms that treat the problem as either a link-prediction in a tripartite graph and exploits the Katz measure to improve ranking [22] or weighted directed graph which models the informational channels of a folksonomy and exploits the PageRank ranking algorithm [21]. Similarly, Wetzker et al. [27] proposed a user-centric tag model that applies a 3-order tensor to model the association between multimedia users, tags, and items in order to infer the meaning of user-assigned tags and personalize the recommendation process.

These approaches took important steps towards improving multimedia item recommendations. Our approach, however, is different in several ways. Specifically, our model and its embedded mechanisms process multimedia contents in order to identify threats and vulnerabilities. This is done by capturing the analytical reasoning process of cyber analytics. As such, the contextual information that we exploit in our work is inherently different as it involves the understanding of the fine-grained cognitive process of cyber analysts in the context of Cyber SA.

2.2 Cyber SA analytics

Analysts perform complicated analytical reasoning in different stages of analysis by leveraging their domain knowledge and experience of Cyber SA analytics. Although the duties performed by cyber security analysts are different across institutions, the analytics tasks and responsibilities of analysts are driven by the same goal of achieving Cyber SA [5, 6]. As shown in Fig. 1, data in Cyber SA continues to evolve rapidly and it keeps coming in massive volumes from multiple sources. Furthermore, this data is heterogeneous in nature and therefore cyber analysts employ different techniques to allow them to capture and evaluate the trustworthiness of cyber attack signals. In order to make sense of the collected data, analysts usually conduct a series of analyses to capture the “true signals” from the collected data and categorize them according to the corresponding cyber attack incidents.

As such, many approaches have been proposed in literature that attempt to study and analyze the interaction between cyber analysts and network monitoring data in Cyber SA. These approaches tackle the problem from different perspectives. In this article, however, we focus our attention on those methodologies and tools that attempted to enhance the data analysts’ performance. Mostly, these approaches are based on familiar fields of study, including Human-Computer Interaction (HCI), Artificial Intelligence (AI), and Big Data. However, the available studies of Cognitive Task Analysis (CTA) in Cyber SA provides a good starting point to understand cyber analysts’ work in Cyber SA at a higher level.

CTA is a traditional task analysis method that can be used to study tasks with intensive cognitive activities. These methods analyze and represent the cognitive activities and the actions that people utilize to perform certain tasks or achieve certain goals. Among the available CTA studies in the context of Cyber SA is the work of D’Amico et al. [4], which studied the different types of cyber security analytics withing the U.S Department of Defense and the industry. Specifically, these types include data triage analysis, correlation analysis, escalation analysis, threat analysis, forensic analysis, and incident response. In a later study [5], the authors developed a more comprehensive work-flow of the analysis

Author's personal copy

process which addresses both strategic and tactical goals in the context of Information Assurance(IA). However, due to the fact that CTA studies are quite expensive and time consuming, conducting such studies in the cybersecurity domain is quite impractical.

At the *network event* level, raw network data collected via automated cybersecurity tools such as firewalls, IDS/IPS systems, and vulnerability scanners can be represented as network events. Initially, false alerts or irrelevant logs are singled out using suspicious event detection systems. This is done using the signature matching approach [16, 26] where network data traffic is compared to the existing signatures of malicious patterns or by detecting anomaly using statistical techniques [17, 20]. Although these approaches automate the process slightly, cyber analysts are still required to manually inspect network events to identify credible events. This initial investigation of network events and network monitoring data by the analyst is referred to as *triage analysis* [5].

Once a network event is initially identified as suspicious, it is often escalated for further investigations. Furthermore, the history of prior related events along with patterns are identified. This stage of analysis have been studied by researchers in the form of alert correlation in which alerts are aggregated by their common characteristics such as port number and source/destination IP addresses [3, 9]. Other approaches addressed this problem using heuristics to associate alerts that indicate the same malicious event in a multi-step attack [13, 25]. However, such alert correlation is limited by the fact that it can not analyze data from multiple sources. This is quite a limitation considering the fact that more sophisticated attacks can be coordinated among multiple attackers and arrived from multiple segments of the network.

Analysis at the *incident* level is quite different than analysis at the network event level in that it is meant to obtain a higher-level insight of cyber attacks by focusing on understanding the relationship between incidents [5]. When incidents are confirmed, cyber analysts utilize methods to perform incident correlation. This is done by associating various incidents that may have been detected in totally different locations with the available intelligence information in an attempt to identify the attackers and their true intent. Once an improved understanding is achieved, cyber analysts take responsive incident actions and begin gathering evidence about the attackers [5, 8, 14]. When incidents are confirmed, proactive threat analysis predicts future potential attacks [5].

This line of research in Cyber SA has inspired us to investigate these issues from different perspectives. As such, our proposal is different in that it establishes the connection between multimedia recommendation and Cyber SA and processes data in different types of modality. In other words, the system we describe in the next section is a true multimedia recommendation system that has been designed to be utilized by cyber analysts while investigating threats. This system incorporates ranking methods and contextual information in order to rank and personalize its recommendations for cyber analysts.

3 The recommendation system

In this article, we propose a multi-modal context-aware recommendation system that facilitates Cyber SA analysis. Figure 2 shows the usual interaction between an analyst and the collected Cyber SA data from various sources. This kind of interaction is our primary mean to delve further into the cognitive process of how analysts absorb and process information about possible cyber attacks. Typically, the analyst continues to process the data and update his/her mental model based on the current context. This process is complicated and

Author's personal copy

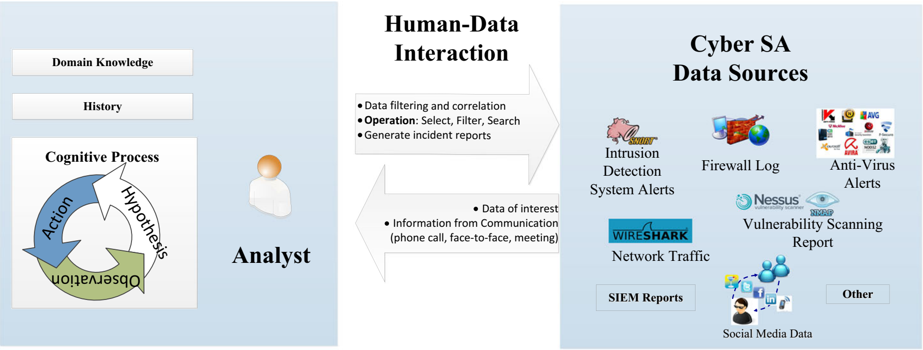

Domain Knowledge
History
Cognitive Process
Action
Hypothesis
Observation
Analyst
Human-Data Interaction
• Data filtering and correlation
• Operation: Select, Filter, Search
• Generate incident reports
• Data of interest
• Information from Communication (phone call, face-to-face, meeting)
Cyber SA Data Sources
Intrusion Detection System Alerts
Firewall Log
Anti-Virus Alerts
Vulnerability Scanning Report
Network Traffic
SIEM Reports
Other
Social Media Data

Fig. 2 The human-data interaction in the multi-modal recommendation system

very time consuming as the data continues to be changed and updated in real time. Therefore, our recommendation system automates this process by capturing the analyst's current context of analysis. This is done by obtaining the information of the analyst's data analysis actions, observations of suspicious data and his/her hypotheses about a possible attack incident. Based on the detected context, the recommendation system searches the analysts' history of analytical processes for similar cases and provides recommendations on the data of interest based on the retrieved history and the analyst's domain knowledge.

There are several benefits for incorporating contextual information in the recommendation process. Firstly, contextual information enables better data selection and *data triage* of the large-scale multimedia data available for considerations. Specifically, data triage is one of the challenging analysis processes that analysts go through because it determines what data is to be considered for further analysis and decision making. Secondly, analyst-system interaction becomes seamless and automatic. This means that the analyst can achieve better recommendations and feedback in a timely manner and with minimal efforts through proper filtering of multimedia data coming from various Cyber SA data sources.

3.1 System architecture

Our recommendation system is designed as a distributed system following the client-server model. It consists of several primary components, including the analyst herself, Cyber SA data, data operation interfaces, a local server, and a cloud-based server. As shown in Fig. 3, the client side implements the interaction between the analyst and the system's interface. The embedded local server in the client side is responsible for data analysis, data storage, and most importantly it implements the recommendation logic through its interfaces. Therefore, the local server acts as a local analysis support agent that interacts with the cyber security analyst. It hosts the multimedia data, the domain knowledge base (KB), analysts' history, and maintains the interaction with a dedicated cloud server.

The server side of the system also includes a cloud server that acts as a support agent for the local server and performs information processing storage. The server cloud runs a number of web services that manage the storage of all multimedia data sources and social interfaces including all the resources and databases available for the local server to query. As such, the cloud server is meant to facilitate the coordination and sharing of resources and services so that the recommendation engine can have all data needed to process.

Author's personal copy

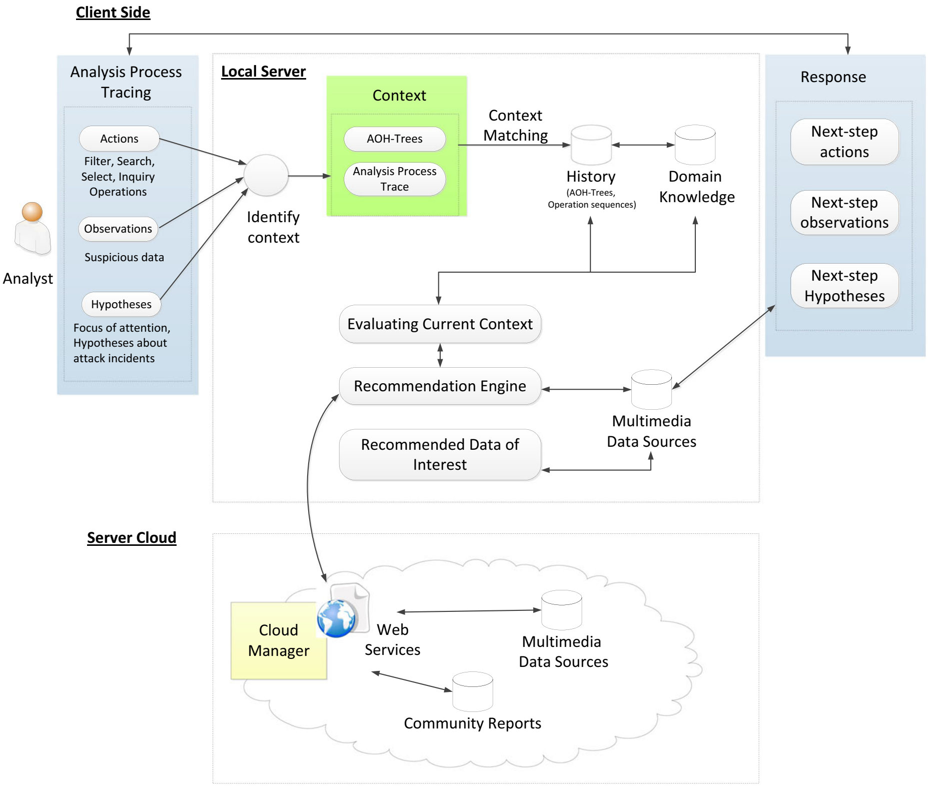


Fig. 3 The high level architecture of the recommendation system

It is worth mentioning that using the cloud for information processing and storage has its own set of risks, but it also has its benefits, including even some security benefits. Therefore, benefits needs to be weighed against the risks that the cloud model brings with it. Some of the known issues with using cloud servers for storage and processing of data include brute-force attacks, bot malware, and data security and privacy [7]. However proper security measures that may include access and configuration management controls alongside with proper vulnerability assessment practices can often mitigate these security risks and provide assurances that cloud data is being stored and processed safely. While security of cloud data is a research field on its own and certainly beyond the scope of this paper [23, 24], it should be known that besides the just mentioned security measures, our cloud server is meant to be deployed such that multi-tenancy, authentication, and trust issues are considerably reduced through the use of dedicated servers that are rigorously monitored and logged.

The core component of the recommendation system is the recommendation engine, which is equipped with reasoning capabilities that allows it to execute the recommendation logic and personalize the recommendations to the analyst. Given the current context of an analyst's analytical process, the recommendation engine searches for analysis operations with similar contextual information from the historical traces of the analysts' analytical processes. To support the search process, the engine collects contextual data and provides reasoning capabilities to match and rank the recommendations based on the current contexts.

Author's personal copy

3.1.1 Analytical process tracing component

The proposed system adopts the trace representation of an analyst's analytical process of Cyber SA data analysis [29, 31]. An analytical process is a complicated cognitive process involving three key components: (1) *actions* of the data analysis operations, such as data filtering and data correlation, (2) *observations* of suspicious data, and (3) *hypotheses* generated by the analyst about potential attack incidents. The analytical process can be viewed as an iterative loop of an analyst's *actions*, *observations* and *hypotheses*: a data exploration action can result in a new observation of suspicious network event; the new observation may trigger more hypotheses of the analyst about the potential attack incidents, so that the analyst may take more actions for further investigation. It has been shown feasible to trace an analyst's analytical process by collecting information of the analyst's *actions*, *observations*, and *hypotheses* [29]. A computer-aided tracing method has been proposed and evaluated in [30].

In the proposed recommendation system, the information about analysts' analytical process is collected by the analytical process tracing component. When an analyst is performing a Cyber SA analytics task, this component captures his/her *actions*, *observations*, and *hypotheses* and their logical relationships. Such relationships can be represented in a tree structure, named "AOH-Trees".

On the right-hand side of Fig. 4, we show an example of a AOH-Tree. In this example, Action 1 resulted in Observation 1, and Hypothesis 1 and Hypothesis 2 were generated by the analyst based on Observation 1. As shown in this figure, an AOH-Tree captures

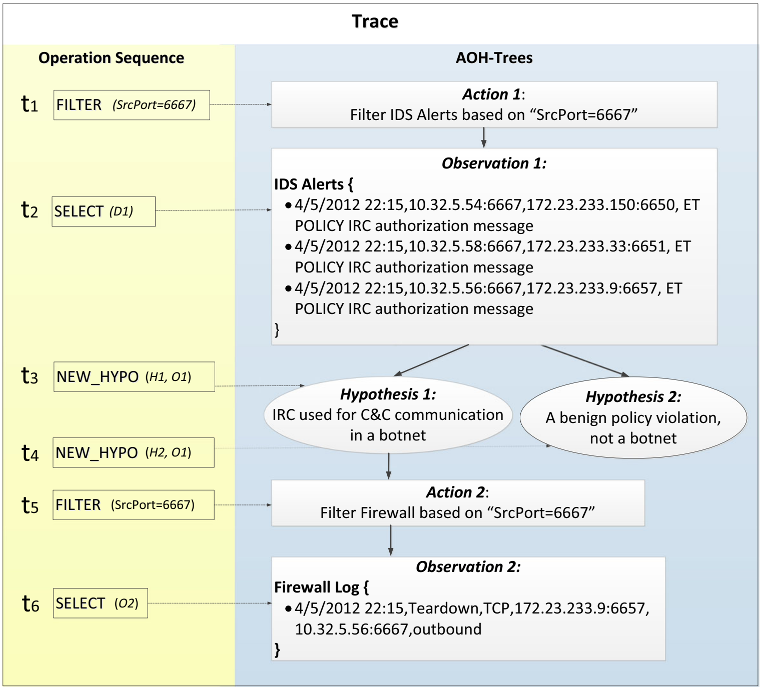

Trace
Operation Sequence
AOH-Trees
t1 FILTER (SrcPort=6667)
t2 SELECT (D1)
t3 NEW_HYPO (H1, O1)
t4 NEW_HYPO (H2, O1)
t5 FILTER (SrcPort=6667)
t6 SELECT (O2)
Action 1: Filter IDS Alerts based on "SrcPort=6667"
Observation 1:
IDS Alerts {
• 4/5/2012 22:15,10.32.5.54:6667,172.23.233.150:6650, ET POLICY IRC authorization message
• 4/5/2012 22:15,10.32.5.58:6667,172.23.233.33:6651, ET POLICY IRC authorization message
• 4/5/2012 22:15,10.32.5.56:6667,172.23.233.9:6657, ET POLICY IRC authorization message
}
Hypothesis 1: IRC used for C&C communication in a botnet
Hypothesis 2: A benign policy violation, not a botnet
Action 2: Filter Firewall based on "SrcPort=6667"
Observation 2:
Firewall Log {
• 4/5/2012 22:15,Teardown,TCP,172.23.233.9:6657, 10.32.5.56:6667,outbound
}

Fig. 4 An example of a trace: operation sequence and AOH-Trees

Author's personal copy

the logical relationships between *actions*, *observations*, and *hypotheses*. Additionally, we also consider the analysts' analysis operations in temporal order. Therefore, we capture analysts' operation sequences in time order whereas each operation is defined by its type and the needed details. Figure 4 also demonstrates an operation sequence corresponding to the AOH-Tree on the right. In Fig. 4, there are four operations occurred at different time points, t_1, t_2, t_3 and t_4. Operations at t_1 and t_2 correspond to $Action1$ and $Observation1$ respectively. Subsequently, the analyst first generated a new hypotheses (Hypothesis 1) and then generated another alternative hypothesis (Hypothesis 2) at times t_3 and t_4, respectively.

The captured operation sequence and AOH-Trees are called a "**trace**", which captures both the logic and temporal relationships between an analyst's *actions*, *observations*, and *hypotheses*. The current **context** of an analyst refers to the current status of the analyst's analytical process. Therefore, the context is defined as the current operation sequence and the current AOH-Trees.

3.1.2 Response component

The response component of the system presents the recommendation results to analysts. Once the matching of historical traces of analytical processes are identified, they are further ranked according to the similarity of contexts. Given the matched historical traces, we further extract the analysts' focus of attention in their following analysis steps to identify the characteristics of the data of interest in those cases. Based on the data characteristics, we can further identify the data of interest in the current Cyber SA data sources and recommend them to the analyst.

3.2 System features

3.2.1 Context-aware system

As the focus of the recommendation system is to recommend Cyber SA data to an analyst, it is important to determine what is the data of interest. Recall that the goal of data analysis is to filter out the irrelevant data and correlate the data that indicates a similar attack. Therefore, the data of interest for an analyst who is performing a Cyber SA analysis task refers to the data which is relevant to his/her focus of attention and can provide new clues of attack incidents. Therefore, as described in Section 3.1.1, the concept of context in this paper mainly refers to the context of an analyst's analytical process, which is defined by the analyst's actions, observations, hypotheses and their relationships.

3.2.2 Seamless interaction

Cyber security analysts need to be highly focused on their data analytics tasks. Therefore, the recommendation system is designed as a system that does not require much user's attention. The analytical process tracing component of the system collects the contextual information by tracing analysts' analytical processes in a minimum reactive way. Once recommendations are provided to an analyst considerations, the system keeps track of the analysts' analytical process. If the analyst select the recommended data as his/her observations of suspicious events, it is viewed as a positive feedback of the previous recommendation. Otherwise, if the analyst does not pay any attention to the recommended items, the system takes it as a negative feedback. In this way, the system requires minimal effort for analysts to provide feedback.

Author's personal copy

4 Recommendation model

In this section, we present a formalization of our recommendation model. In particular, in the following subsection, we formulate the problem using various sets that represent the different facets in the recommendation model. In particular, we define the sets of dimensions, events, contexts, and analysts. In Section 4.2 we formally present the model we use that expresses the relationships between these sets.

4.1 Preliminary definitions

Our recommendation system is backed by a formal model that assists cyber analysts with identifying and retrieving multimedia items that contain traces of cyber threats. The recommendations are based on contextual information and analysts' personal preferences. As such, our model is composed of the following sets of distinct elements:

Dimensions Set $D = \{d_1, \ldots, d_n\}$ *where* n *is the number of dimensions*: This set represents the characteristics of Cyber SA data that includes elements such as time, source IP, destination IP, source port, destination port, direction, priority, and alert message.
Items or Events Set $I = \{i_1, \ldots, i_m\}$ *where* m *is the number of events(items)*: The Cyber SA data sources is modeled as a set of events with certain characteristics, where an item $i_j(1 \leq j \leq m)$ specifies a value in each dimension of set D, thus specifying the event characteristic.
Contexts Set $C = \{c_1, \ldots, c_z\}$ *where* z *is the number of contexts*: The concept of context is defined by an analyst's analytical process, involving actions, observations, and hypotheses, which specify the current focus of attention of the analysts. In this set, a context, $c_j(1 \leq i \leq z)$ represents an attribute of the context in the dimension d_j.
Analysts Set $A = \{a_1, \ldots, a_x\}$ *where* x *is the number of analysts*: This set represents the historical data of the previously captured analytical processes by former analysts

The use of these sets in the recommendation process can be simply characterized as follows: Suppose the current analyst is a, the task of the recommendation system is to recommend Cyber SA data set I to a by matching the current context c_j of the analyst a from the historical analytical processes of the analysts in set A. In the following subsection, we characterize the relationships among these sets and describe our recommendation algorithm.

4.2 Recommendation model

Using the four sets D, I, C, and A that we defined previously, we construct the following matrices to represent the relationships among analysts, contexts, and items.

Analyst-Context Matrix $\mathbf{S}_{a,c}$: This matrix shapes the relationship between analysts and contexts through an aggregation task over (A, C).

$$\mathbf{S} = \begin{bmatrix} f_S(a_1, c_1) & \ldots & f_S(a_1, c_z) \\ \vdots & \ddots & \vdots \\ f_S(a_x, c_1) & \ldots & f_S(a_x, c_z) \end{bmatrix} \tag{1}$$

Where $f_S(a, c)$, $1 \leq a \leq x$, $1 \leq c \leq z$ is the frequency of the context c occurred in the traces of analyst a's analytical process.
Analyst-Item Matrix $\mathbf{B}_{a,i}$: This matrix represents the relationships between analysts and items, for each pair of (a, i), we extract the frequency of the analyst a selected the item

Author's personal copy

i as an observation of suspicious event. Using the frequency values, the matrix $\mathbf{B}_{a,i}$ can be built as follows:

$$\mathbf{B} = \begin{bmatrix} f_B(a_1, i_1) & \dots & f_B(a_1, i_m) \\ \vdots & \ddots & \vdots \\ f_B(a_x, i_1) & \dots & f_B(a_x, i_m) \end{bmatrix} \tag{2}$$

Where $f_B(a, i), 1 \leq a \leq x, 1 \leq i \leq m$ is the frequency of item i being selected by analyst a as observations of suspicious events.

Context-Item Matrix $\mathbf{E}_{c,i}$: This matrix represents the relationships between contexts and items. This matrix can be constructed by aggregating over (C, I)

$$\mathbf{E} = \begin{bmatrix} f_E(c_1, i_1) & \dots & f_E(c_1, i_m) \\ \vdots & \ddots & \vdots \\ f_E(c_z, i_1) & \dots & f_E(c_z, i_m) \end{bmatrix} \tag{3}$$

Where $f_E(c, i), 1 \leq c \leq z, 1 \leq i \leq m$ is the frequency of item i appeared in context c.

Context-Context Similarity Matrix $\mathbf{F}_{c,c}$: This matrix allows us to match contexts by computing the similarity between each pair of contexts. This matrix is constructed by decomposing the Context-Item matrix $\mathbf{E}_{c,i}$. Given a pair of contexts c_p and c_q, we find the items consumed in each given context. The similarity value of c_p and c_q is calculated by counting the frequency of the consumption of an item for the pair of contexts, or by using a binary function. We further measure the *cosine* angle between the two computed values for all items consumed in one context compared to another. The following is the definition of $\mathbf{F}_{c,c}$.

$$\mathbf{F} = \begin{bmatrix} f_F(c_1, c_1) & \dots & f_F(c_1, c_z) \\ \vdots & \ddots & \vdots \\ f_F(c_z, c_1) & \dots & f_F(c_z, c_z) \end{bmatrix} \tag{4}$$

Where $f_F(c, c), 1 \leq c \leq z$ is the similarity value between a pair of contexts. The similarity value can be measured as the *cosine* angle value between a pair of contexts vectors p and q as follows:

$$f_F(c_p, c_q) = cos(c_p, c_q) = \frac{c_p \cdot c_q}{||c_p||^2 \times ||c_q||^2} \tag{5}$$

Item-Item Similarity Matrix $\mathbf{G}_{i,i}$: This matrix allows us to trace the relationship between different items consumed by the analysts. Accordingly, we build the Item-Item similarity matrix $\mathbf{G}_{i,i}$ by computing the similarity between two items from matrix $\mathbf{B}_{a,i}$.

$$\mathbf{G} = \begin{bmatrix} f_G(i_1, i_1) & \dots & f_G(i_1, i_m) \\ \vdots & \ddots & \vdots \\ f_G(i_m, i_1) & \dots & f_G(i_m, i_m) \end{bmatrix} \tag{6}$$

Where $f_G(i, i), 1 \leq i \leq m$ is the similarity value between a pair of items. The similarity value can be measured as the *cosine* angle value between a pair of items vectors p and q as follows:

$$f_G(i_p, i_q) = cos(i_p, i_q) = \frac{i_p \cdot i_q}{||i_p||^2 \times ||i_q||^2} \tag{7}$$

4.3 Ranking of candidate recommendations

Depending on the breadth and depth of the historical analytical processes that the system is currently processing, recommending items from the Cyber SA data set to an analyst based

Author's personal copy

on the current analyst's context can produce multiple recommended items. Therefore, our system provides a mechanism to rank the recommended items based on their degree of relevancy to the current situation.

Our ranking procedure utilizes the matrices we just constructed and further identifies the *latent associations* between both analysts and contexts as well as the latent associations between analysts and items. In particular, we utilize the *transpose* of the two matrices $\mathbf{F}_{c,c}$ and $\mathbf{G}_{i,i}$. More specifically, by multiplying the two matrices $\mathbf{S}_{a,c} \times \mathbf{F}^{T}_{c,c}$ and $\mathbf{B}_{a,i} \times \mathbf{G}^{T}_{i,i}$ respectively, we can obtain two latent matrices that we can use to define the ranking.

For a given detected context c, the ranking score of an item i for an analyst a is obtained using the following equation:

$$\mathbf{Rank}_{a,c}(i) = \sum_{j=1}^{z}(\mathbf{S}_{a,j} \times \mathbf{F}^{T}_{c,j}) \times \sum_{j=1}^{m}(\mathbf{B}_{c,j} \times \mathbf{G}^{T}_{i,j}) \tag{8}$$

5 Evaluation

In order to investigate and evaluate the value of our context-adaptive approach, we have implemented a prototype that embodies the logic of our recommendation model. This prototype allows analysts to inspect and identify incidents by searching large volumes of Cyber SA data sets. This tool is also capable of storing and indexing the strategies utilized by expert cyber analysts while dealing with an attack incident. The captured knowledge enriches the existing knowledge-base and can be used for future recommendations of similar attack incidents. Furthermore, the prototype allows analysts to enter contextual information about the current captured incident.

Using this prototype, we have conducted multiple experiments and case studies. In this section, we report the results of one of the major case studies that we have conducted to assess how our recommendation model benefits cyber analysts in identifying potential threats in Cyber SA multimedia data sources.

The fundamental hypotheses we test in this Human-in-the-Loop case study are:

H 1 *Our methods for capturing the fine-grained traces of the cognitive processes of cyber analysts aid decision making in Cyber SA through threat understanding, analysis, and risk assessment.*

H 2 *Our recommendation algorithm improves precision of threat identification and enhances the filtering and ranking of the recommended items.*

H 3 *Incorporating context-adaptive techniques personalize multimedia recommendations.*

In order to carry out this experiment, a history database that contains traces of analysts' cognitive process in Cyber SA was needed to be constructed. The process of constructing this database of analytical processes is described next.

5.1 History database setup

In order to evaluate the proposed recommendation system, a history database that captures cyber analysts' operation traces while they are performing cyber analysis tasks is required.

Author's personal copy

To ensure a valid and effective evaluation, we constructed the history database following these principles:

- P1: instances in the database (i.e., "traces") should be **representative** traces. More specifically, the analytical processes represented by the traces should reflect the typical analytical reasoning activities and strategies of analysts in the real world.
- P2: a **variety** of analytical processes should exist considering that the history database contains the traces of analysts who perform Cyber SA analytics differently.
- P3: the database should contain **sufficient** instances.

Using these three principles as our guide, we have built the history database by generating simulated traces of analytical processes. The traces were simulated by referring to traces which were collected in a project with cyber defense analysts and Ph.D. students specialized in cyber security [29, 31]. The students involved in the project possess enough expertise and knowledge in cyber security analysis. It has been verified that the collected traces capture the key activities of analysts' analytical processes and therefore various analytical processes were implied in the collected traces [29]. Using these traces as the "seeds", we constructed the history database by generating 150 derivatives from these seeds. Following principles P1, P2 and P3 as our guide, the derivatives were generated by adding variations to the original seed traces. The variations include (1) adding observations into the traces, (2) splitting a trace into multiple traces, and (3) combining the parts from different traces into one trace.

5.2 Case study

We conducted a case study to evaluate the performance of the recommendation algorithm. Seven traces were randomly selected from the history database. These traces are denoted by T1 (the trace shown previously in Fig. 4), T2, T3, T4, T5, T6, and T7. Using these traces, seven experiments were conducted. In each experiment, one trace was used as the query trace and the remaining six traces were viewed as the history.

Given the query trace and the remaining historical traces, we evaluated the recommendation algorithm in the following manner. Initially, we identified the current context in the query trace. Using this context, we matched it with the remaining historical traces using our recommendation model. The historical traces were further ranked according to the similarity between them and the current context. Furthermore, we asked two specialized individuals to rank the historical traces as the ground truth. Using this ground truth, we evaluated the performance of the recommendation algorithm by comparing the system's output with the ground truth.

When determining the degree of similarity between two traces, we mainly focused on the data items included in the *observations* in these traces and calculate the *cosine* similarities as described by our recommendation model.

To illustrate our procedure, let us assume that the trace shown previously in Fig. 4 is trace T1. Let us also assume that the context of this trace is the current context. We then proceed by using our algorithm to match T1 with traces T2, T3, T4, T5, T6, and T7. This process revealed that T4, which is shown in Fig. 5 is the best match. The calculated cosine similarity score is 0.5669467, which was the highest among other obtained similarity scores we obtained. Manual inspection by specialists of the other traces revealed that T4 was indeed the best match based on the ground truth ranking. Thus, providing evidence that support hypotheses H2 and H3. The similarities between T1 and the other six traces are demonstrated in Fig. 6.

Author's personal copy

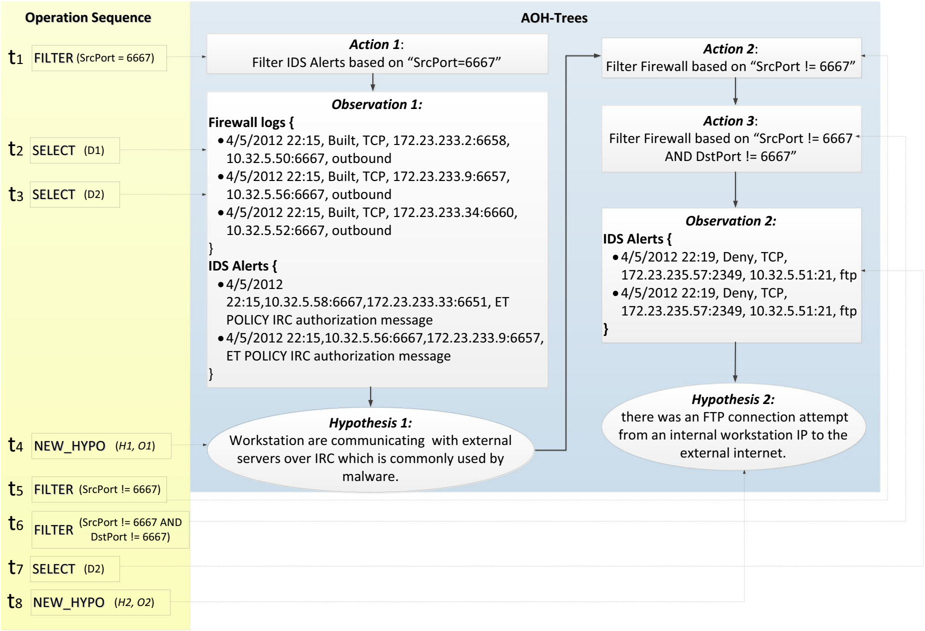

Operation Sequence
t1 FILTER (SrcPort = 6667)
t2 SELECT (D1)
t3 SELECT (D2)
t4 NEW_HYPO (H1, O1)
t5 FILTER (SrcPort != 6667)
t6 FILTER (SrcPort != 6667 AND DstPort != 6667)
t7 SELECT (D2)
t8 NEW_HYPO (H2, O2)
AOH-Trees
Action 1: Filter IDS Alerts based on "SrcPort=6667"
Observation 1:
Firewall logs {
•4/5/2012 22:15, Built, TCP, 172.23.233.2:6658, 10.32.5.50:6667, outbound
•4/5/2012 22:15, Built, TCP, 172.23.233.9:6657, 10.32.5.56:6667, outbound
•4/5/2012 22:15, Built, TCP, 172.23.233.34:6660, 10.32.5.52:6667, outbound
}
IDS Alerts {
•4/5/2012 22:15,10.32.5.58:6667,172.23.233.33:6651, ET POLICY IRC authorization message
•4/5/2012 22:15,10.32.5.56:6667,172.23.233.9:6657, ET POLICY IRC authorization message
}
Hypothesis 1: Workstation are communicating with external servers over IRC which is commonly used by malware.
Action 2: Filter Firewall based on "SrcPort != 6667"
Action 3: Filter Firewall based on "SrcPort != 6667 AND DstPort != 6667"
Observation 2:
IDS Alerts {
•4/5/2012 22:19, Deny, TCP, 172.23.235.57:2349, 10.32.5.51:21, ftp
•4/5/2012 22:19, Deny, TCP, 172.23.235.57:2349, 10.32.5.51:21, ftp
}
Hypothesis 2: there was an FTP connection attempt from an internal workstation IP to the external internet.

Fig. 5 The trace T4 that matched T1 shown in Fig. 4 best

The similarity ranking can be validated by the ground truth gained based on the understanding of the two traces. Observation 1 in T4 contains the same IDS alerts of Observation 1 in T1. More specifically, when our system detected that T1 is the current context, it has recommended to the analyst trace T4 as a matching context. In other words, the analyst who is using our system has essentially found the malicious IRC communication events, which shows support for hypothesis H1.

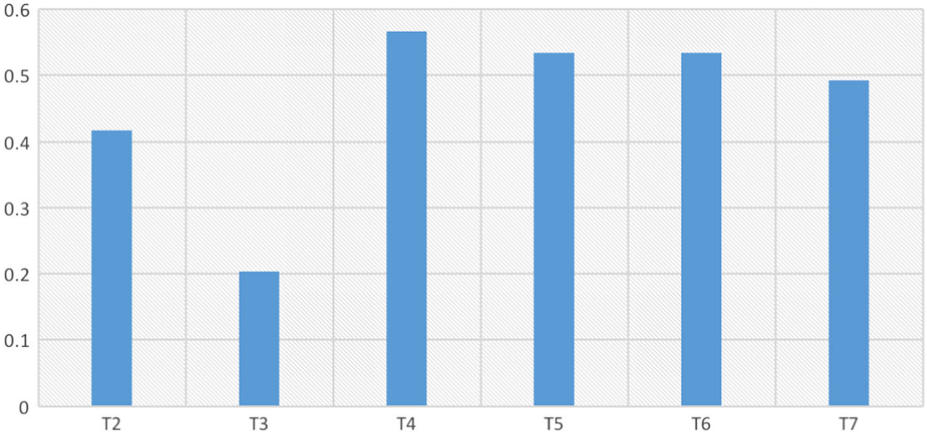


Fig. 6 The similarity between T1 and the other six traces (T2, T3, T4, T5, T6 and T7)

Author's personal copy

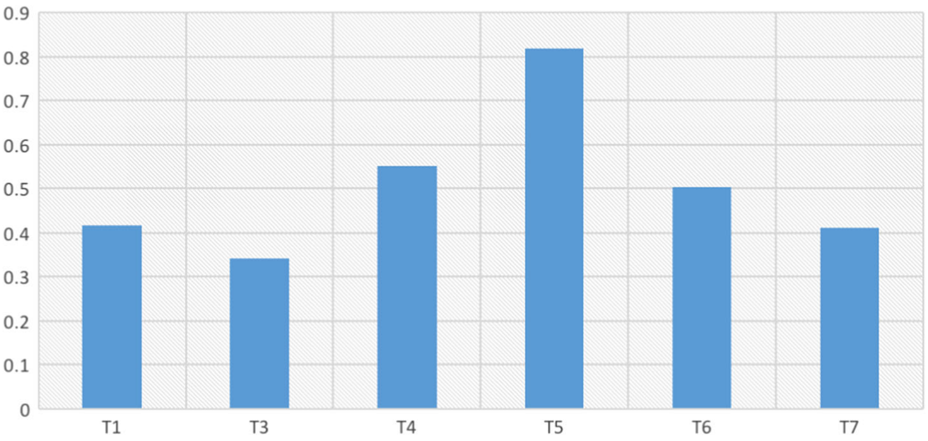


Fig. 7 The similarity between T2 and the other six traces (T1, T3, T4, T5, T6 and T7)

We have conducted six more similar experiments by repeating the same process described above. In each one of these other experiments, a another trace was treated as the query trace. Considering the similarity scores in these seven experiments, the mean of the similarity score is 0.5141 (SD=0.161). After completing all seven experiments, we have found that in all cases but one case, our system provided recommendations and ranking that matches the ground truth. In other words, only one experiment revealed that the top recommended trace did not match the ground truth. In this experiment, we treated T2 as the query trace. We further calculated the similarity between T2 and the other six traces. As shown in Fig. 7, the recommended trace T5 had the highest similarity score, however, the ground truth indicated T6 was the most relevant trace instead of T5.

Given this mismatch, we investigated the reason why T6 had a lower similarity score than T5 according to the similarity algorithm. We found that the *observations* in T6 contains the IRC communications events between a set of external servers (including 10.32.5.52, 10.32.5.54, 10.32.5.56, 10.32.5.57 and 10.32.5.58) and internal workstations in the subnetwork 172.23.233.0, while T2 contains an *observation* including the IRC communication events between the external server 10.32.5.5 and the internal workstations in the subnetwork 172.23.238.0. These two observations had no overlapping events when the system calculated the cosine similarity, thus resulting in a relatively low score. However, they indicated the same type of IRC communication events in a botnet with a large scale of IPs being involved. Therefore, they are relevant according to the ground truth. This mismatch between ground truth and system's output suggested we may need to consider event abstraction at a different level in order to compare observations. Besides, this issue can be resolved by considering the semantic meaning of observations. Regardless, the results of our seven experiments show support to the validity of our hypotheses.

6 Conclusions and future work

The already existing large volumes of multimedia data with various forms of modality needs to be inspected and evaluated for cyber threats. Thus, the work presented in this article uniquely contributes to the proper inclusion and inspection of such data in the context of Cyber SA.

Author's personal copy

As such, we have described the design of a multi-modal recommendation system that promotes and supports Cyber SA. In particular, the system is supported by a cloud server that runs multiple web services to make it capable of analyzing multimedia items from various network data sources in order to filter and identify cyber threats and vulnerabilities. This system assists cyber analysts by personalizing the recommendations based on their current context. More specifically, the recommendation process incorporates a knowledge base of prior operation traces of expert analysts' cognitive process while performing day-to-day cyber analysis tasks and incident identification. Thus, the recommendation model and its embedded algorithm perform a systematic similarity-based matching between current and prior traces based on the gathered contextual information.

This work opens new doors for further enhancements and new research perspectives. As we have seen in the previous section, traces of cyber analysts' previous activities contain valuable cognitive information about best strategies used to deal with cyber incidents. In return, these traces inform future incident identification. However, analyzing these traces is a time-intensive and complex activity. Therefore, an interesting future work direction would be to find ways that makes this process more automatic.

Ontologies describe domain concepts and their relationships concisely. They are also known for their solid and formal reasoning foundation in data modeling and therefore they can be used to structure and build the knowledge base we described in this paper. Therefore, investigating the application of semantic annotations and domain-specific ontologies to provide better matching and ranking of candidate recommendations is foreseen as a promising future work direction.

Interpreting the operations in traces is usually a time-consuming and complex process. We have however observed that there are some patterns of sequential operations in traces. Therefore, a good future work direction would be to study such patterns carefully in an effort to achieve more efficient ways that can automatically perform trace analysis. Finally, the case study we have described in this paper demonstrates the utility of our proposed approach. New experiments are currently being designed and will be conducted involving real representative users in controlled settings. The goal of such experiments is to evaluate the utility and performance of our system and to learn how well potential users perform real-world cyber SA predefined tasks.

Acknowledgements The authors are grateful to the Deanship of Scientific Research, King Saud University for supporting through Vice Deanship of Scientific Research Chairs.

References

1. Alhamid MF, Rawashdeh M, Dong H, Hossain MA, Alelaiwi A, El-Saddik A (2016) RecAm: a collaborative context-aware framework for multimedia recommendations in an ambient intelligence environment. Multimedia Syst 22(5):587–601
2. Chen CC, Huang TC, Park JJ, Yen NY (2015) Real-time smartphone sensing and recommendations towards context-awareness shopping. Multimedia Syst 21(1):61–72
3. Cuppens F, Miege A (2002) Alert correlation in a cooperative intrusion detection framework. In: Proceedings of the IEEE symposium on security and privacy, pp 202–215
4. D'Amico, A, Whitley K, Tesone D, O'Brien B, Roth E (2005) Achieving cyber defense situational awareness: a cognitive task analysis of information assurance analysts. In: Proceedings of the human factors and ergonomics society annual meeting, vol 49, no 3. SAGE Publications, pp 229–233
5. D'Amico A, Whitley K (2008) The real work of computer network defense analysts. In: VizSEC. Springer, Heidelberg, pp 19–37

Author's personal copy

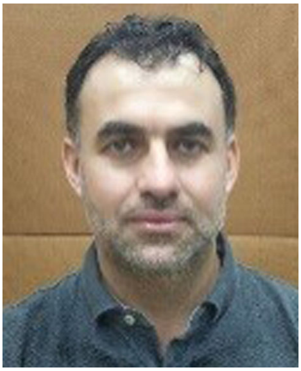
6. Dutt V, Ahn YS, Gonzalez C (2011) Cyber situation awareness: modeling the security analyst in a cyber-attack scenario through instance-based learning. In: Data and applications security and privacy XXV. Springer, Heidelberg, pp 280–292
7. Gupta S, Gupta BB (2016) XSS-secure as a service for the platforms of online social network-based multimedia web applications in cloud. Multimed Tools Appl. doi:10.1007/s11042-016-3735-1
8. Gupta B, Agrawal DP, Yamaguchi S (2016) Handbook of research on modern cryptographic solutions for computer and cyber security. IGI Global, Hershey. doi:10.4018/978-1-5225-0105-3
9. Hervé D, Wespi A (2001) Aggregation and correlation of intrusion-detection alerts. In: Recent advances in intrusion detection. Springer, Berlin Heidelberg, pp 85–103
10. Hossain MS, Hossain SKA, Alamri A, Hossain MA (2013) Ant-based service selection framework for a smart home monitoring environment. Multimed Tools Appl 67(2):433–453
11. Hossain MA, Alamri A, Alhamid MF, Rawashdeh M, Alnusair A (2014) Collaborative recommendation of ambient media services. In: IEEE International Conference on Multimedia and Expo Workshops (ICMEW), pp 1–6
12. Hossain MS, Muhammad G, Rahman SkMM, Abdul W, Alelaiwi A, Alamri A (2016) Toward end-to-end biometrics-based security for IoT infrastructure. IEEE Wirel Commun Mag 23(5):44–51
13. Julisch K (2003) Clustering intrusion detection alarms to support root cause analysis. ACM Trans Inf Syst Secur (TISSEC) 6(4):443–471
14. Killcrece G, Kossakowski KP, Ruefle R, Zajicek M (2003) State of the practice of computer security incident response teams (CSIRTs). No. CMU/SEI-2003-TR-001. Carnegie Mellon University. Pittsburgh, Software Engineering Inst
15. Kim J, Lee D, Chung KY (2014) Item recommendation based on context-aware model for personalized u-healthcare service. Multimed Tools Appl 71(2):855–872
16. Kumar S, Spafford EH (1994) A pattern matching model for misuse intrusion detection. In: Proceedings of the 17th national computer security conference
17. Mukherjee B, Heberlein LT, Levitt KN (1994) Network intrusion detection. IEEE Netw 8(3):26–41
18. Pappas N, Popescu-Belis A (2015) Combining content with user preferences for non-fiction multimedia recommendation: a study on TED lectures. Multimed Tools Appl 74(4):1175–1197
19. Pombinho P, Carmo MB, Afonso AP (2012) Context aware point of interest adaptive recommendation. In: Proceedings of the 2nd workshop on context-awareness in retrieval and recommendation, pp 30–33
20. Portnoy L, Eskin E, Stolfo SJ (2000), Intrusion detection with unlabeled data using clustering. J Inf Secur. doi:10.4236/jis.2011.24016
21. Ramezani M (2011) Improving graph-based approaches for personalized tag recommendation. J Emerg Technol Web Intell 3(2):168–176
22. Rawashdeh M, Alhamid MF, Alja'am JM, Alnusair A, El-Saddik A (2016) Tag-based personalized recommendation in social media services. Multimed Tools Appl 75(21):13299–13315
23. Rebolloa O, Melladob D, Fernández-Medinac E, Mouratidisd H (2015) Empirical evaluation of a cloud computing information security governance framework. Inf Softw Technol 44–57. doi:10.1016/j.infsof.2014.10.003
24. Stergiou C, Psannis KE, Kim BG, Gupta B (2016) Secure integration of IoT and Cloud Computing. Future Generation Computer Systems, Elsevier
25. Tabia K, Benferhat S, Leray P, Mé L (2011) Alert correlation in intrusion detection: combining AI-based approaches for exploiting security operators' knowledge and preferences. In: Association for the advancement of artificial intelligence, pp 1–8
26. Wang K, Cretu G, Stolfo SJ (2005) Anomalous payload-based worm detection and signature generation. In: Recent advances in intrusion detection. Springer, Heidelberg, pp 227–246
27. Wetzker R, Zimmermann C, Bauckhage C, Albayrak S (2010) I tag, you tag: translating tags for advanced user models. In: Proceedings of the 3rd ACM international conference on Web search and data mining, pp 71–80
28. Zhang Z, Sun R, Zhao C et al (2016) CyVOD: a novel trinity multimedia social network scheme. Multimed Tools Appl. doi:10.1007/s11042-016-4162-z
29. Zhong C, Yen J, Liu P, Erbacher RF, Etoty R, Garneau C (2015) An integrated computer-aided cognitive task analysis method for tracing cyber-attack analysis processes. In: Proceedings of the 2015 symposium and bootcamp on the science of security. ACM, p 9
30. Zhong C, Yen J, Liu P, Erbacher R, Etoty R, Garneau C (2015) ARSCA: a computer tool for tracing the cognitive processes of cyber-attack analysis. In: IEEE international inter-disciplinary conference on cognitive methods in situation awareness and decision support (CogSIMA), pp 165–171
31. Zhong C, Yen J, Liu P, Erbacher RF, Etotyv R, Garneau C (2016). Studying analysts data triage operations in cyber defense situational analysis. In: Liu P, Jajodia S, Wang C (eds) Recent advances in Cyber SA. Springer, LNCS vol 10030

Author's personal copy

Awny Alnusair is currently an associate professor of Informatics and computer science at Indiana University Kokomo. Prior to that, he worked as a lecturer at Northwestern University and a senior fellow at Robert Morris University. He also worked for several years in the software development industry. Dr. Alnusair received a Ph.D. in Computer Science from the University of Wisconsin-Milwaukee. Dr. Alnusair's general research interests generally include software maintenance, multimedia information retrieval, programming languages, and data mining.

Chen Zhong is an assistant professor of Informatics and Computer Science at Indiana University, Kokomo, USA. She received her Ph.D. degree from the School of Information Sciences and Technology at Penn State University. Before to that, Dr. Zhong received her Bachelor degree from the Department of Computer Science at Nanjing University, China. Dr. Zhong's research interests span the areas of cybersecurity (cybersecurity analytics, cyber operations), artificial intelligence (knowledge representation and engineering, case-based reasoning, constraint satisfaction), cognitive modeling (sensemaking and information-seeking), and human-computer interaction (interactive tool design and development, process tracing, human subject study).

Author's personal copy



Majdi Rawashdeh received his Ph.D. degree in Computer Science from the University of Ottawa, Canada. He is currently an Assistant Professor at Princess Sumaya University for Technology (PSUT), Jordan. His research interests include, social media, user modeling, recommender systems, smart cities, and big data.

M. Shamim Hossain is an Associate Professor at the King Saud University, Riyadh, KSA. Dr. Hossain received his Ph.D. in Electrical and Computer Engineering from the University of Ottawa, Canada. His research interests include serious games, social media, IoT, cloud and multimedia for healthcare, smart health, and resource provisioning for big data processing on media clouds. He has authored and coauthored around 120 publications including refereed IEEE/ACM/Springer/Elsevier journals, conference papers, books, and book chapters. He has served as co-chair, general chair, workshop chair, publication chair, and TPC for over 12 IEEE and ACM conferences and workshops. He was the recipient of a number of awards including, the *Best Conference Paper Award*, the *2016 ACM Transactions on Multimedia Computing, Communications and Applications (TOMM) Nicolas D. Georganas Best Paper Award*, and the *Research in Excellence Award* from King Saud University. He is on the editorial board of *IEEE Access*, *Computers and Electrical Engineering (Elsevier), Games for Health Journal*, and *International Journal of Multimedia Tools and Applications (Springer)*. Currently, he serves as a lead guest editor of *IEEE Communication Magazine, IEEE Transactions on Cloud Computing*, *IEEE Access* and *Sensors (MDPI)*. Previously, he served as a guest editor of *IEEE Transactions on Information Technology in Biomedicine (currently JBHI)*, *International Journal of Multimedia Tools and Applications (Springer)*, *Cluster Computing (Springer)*, *Future Generation Computer Systems (Elsevier)*, Computers and Electrical Engineering (Elsevier), and *International Journal of Distributed Sensor Networks*. Dr. Shamim is a Senior Member of IEEE, a member of ACM and ACM SIGMM.

Author's personal copy

Atif Alamri is an associate professor of Information Systems Department, College of Computer and Information Sciences, King Saud University. Riyadh, Saudi Arabia. He has obtained his PhD. From the University of Ottawa, Canada. He was a guest editor of the IEEE Transactions on Instrumentation and Measurement. He has also served as, chair, and technical program committee member in numerous international conferences/workshops like the IEEE International Workshop on Multimedia Services and Technologies for E-health, 10th IEEE International Symposium on Haptic Audio Visual Environments and Games, His research interests include multimedia assisted health systems, ambient intelligence, and service-oriented architecture. He is a member of the IEEE.