

Chapter 12

A Comprehensive Survey of Event Analytics

T. Gidwani

AUT University, New Zealand

W. Yan

AUT University, New Zealand

M. J. Argano

AUT University, New Zealand

F. Issa

AUT University, New Zealand

ABSTRACT

Analytics has emerged as an important area of study as it avoids further incidents or risks after the events have occurred; this is done by analysing computer events and making further statistics. The purpose of this survey is to gain knowledge for the authors' own event knowledge database which will consist of how unusual events work and how they are related to other events. The algorithms mentioned in this paper have been used to build their future development, resulting in a knowledge database designed to be similar to an internet browser engine where it can search events and their relationships. The research and algorithms have helped the authors to decide on the technology they will be using for the knowledge database.

1. INTRODUCTION

An event is an occurrence within a computer system that converses with other systems or users. Computer and network systems contain event logs that holds enormous amount of data. These event logs hold records of any behaviors or actions a network device performs. Events may also involve illegal activities such as malicious attacks or unexpected data movement. The plan is to assemble these events and to examine their

relationships with research and recording each activity into a knowledge database. This information will help avoid further incidents or risks after events have occurred.

Event analytics is a complex scheme therefore we have created subcategories for our research. We divided this into four major components: computer event surveillance, computer event monitoring, computer event forensic and computer event security. In this paper, we have combined computer event surveillance and computer event monitoring

DOI: 10.4018/978-1-4666-4006-1.ch012

together and computer event forensic and computer event security together shown on Figure 1. An extensive research was conducted throughout these subcategories. We have selected the articles written by professionals in their respected fields.

This paper will be divided into four sections: Section 2 will be on state of the arts, which is the highest level of development or technique at this time, a range of systems and techniques will be introduced here. Section 3 will be on existing systems and algorithms. The last section will then be the conclusion that will encapsulate our insights on what was useful and what we have learnt from this research.

2. THE STATE OF THE ARTS

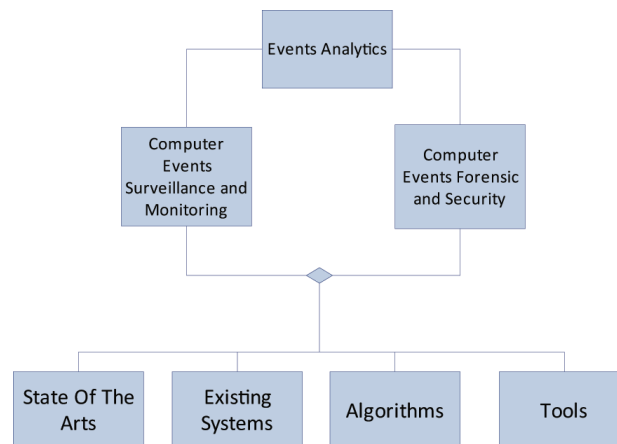
This section covers the highest level of development of computer analytics; it includes topics such as computer surveillance systems, computer forensic events, monitoring events and network events security related methodologies, which are currently being employed. This section contains up to date ideas and knowledge of computer analytics, which can help to make advancements in already existing methodologies.

2.1. Event Based Surveillance and Monitoring

In surveillance, events retrieved from video, audio and image sensors (Bolderheij, Absil, & Genderen, 2005; Gonzalez, 2007; Guennoun, Khattak, Kapralos, & El-Khatib, 2008; Bouhats, Marebati, & Mokhatr, 2007). The purpose does not focus mainly on event detection; instead it focuses more on the event itself. In order to improve unusual event detection, all events must be analyzed individually and categorized based on type. The events are stored in a database to compare relationships for future use, so it can be retrieved when needed. If all events that are recorded and examined are logged into a database it can be used as an event library.

By collecting these events we can examine the reasons of occurrence in which comparisons can be made so as to what events are normal and which ones are not. The application is very similar to youtube and is made to be used by anyone so using the application for the first time should be straight forward (Hameed & Abdullah, 2008; Hannemann, Donohue, & Dietz, 2007; Kieran & Yan, 2010).

Figure 1. Structure of event analytics



13 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/comprehensive-survey-event-analytics/75671

Related Content

Genetic Testing and Protection of Genetic Privacy: A Comparative Legal Analysis in Europe and Australia

Sergio Romeo-Malanda, Dianne Nicol and Margaret Otlowski (2012). *Cyber Crime: Concepts, Methodologies, Tools and Applications* (pp. 1756-1777).

www.irma-international.org/chapter/genetic-testing-protection-genetic-privacy/61036

Advances in Forensic Geochemistry

Elhoucine Essefi (2022). *Technologies to Advance Automation in Forensic Science and Criminal Investigation* (pp. 1-14).

www.irma-international.org/chapter/advances-in-forensic-geochemistry/290643

The Impact of Social Engineer Attack Phases on Improved Security Countermeasures: Social Engineer Involvement as Mediating Variable

Louay Karadsheh, Haroun Alryalat, Ja'far Alqatawna, Samer Fawaz Alhawari and Mufleh Amin AL Jarrah (2022). *International Journal of Digital Crime and Forensics* (pp. 1-26).

www.irma-international.org/article/the-impact-of-social-engineer-attack-phases-on-improved-security-countermeasures/286762

On Steganalysis and Clean Image Estimation

Christopher B. Smith and Sos S. Aghaian (2009). *Multimedia Forensics and Security* (pp. 212-244).

www.irma-international.org/chapter/steganalysis-clean-image-estimation/26995

Detection of Phishing in Internet of Things Using Machine Learning Approach

Sameena Naaz (2021). *International Journal of Digital Crime and Forensics* (pp. 1-15).

www.irma-international.org/article/detection-of-phishing-in-internet-of-things-using-machine-learning-approach/272830