The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM)
ISSN: 2602-3199

The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM), 2022

Volume 18, Pages 1-6

ICBASET 2022: International Conference on Basic Sciences, Engineering and Technology

Data Analytic for Cyber Security: A Review of Current Framework Solutions, Challenges and Trends

Shereen KHAN
Multimedia University

Tan Swee Leng OLIVIA
Multimedia University

Nasreen KHAN
Multimedia University

Ng Kok WHY
Multimedia University

Tan Swee WEI
Multimedia University

Abstract: In context of technology, cybersecurity has seen vital technological and operational developments in recent years, with information science at the forefront of the revolution. The key in creating a complicated and automatic security system is extracting network activity patterns or cybersecurity information insights and constructing an identical data-driven model. The applying of a spread of scientific methodology, machine learning techniques, processes, and systems; information science is to grasp and analyse actual occurrences with information. During this analysis, the researchers consider and in short justify cybersecurity information science, during which information is obtained from relevant cybersecurity sources as well as legislations and analytics are wont to supplement the most recent data-driven trends to supply more practical security solutions. The paradigm of cybersecurity information science, in distinction to standard cybersecurity computing techniques, permits for more practical and complex computing. Researchers check and highlight variety of connected analysis topics and future directions. Additionally, researchers propose a multi-layered framework for cybersecurity modelling. Overall the target is to target the connection of data-driven deciding framework model for safeguarding systems from cyber-attacks, instead of simply discussing cybersecurity information science and applicable approaches.

Keywords: Cyber security, cybercrime, data analytic, legislations

Introduction

Data analytics is a strategy for ensuring accurate data analysis, cleansing, altering, and modelling via the application of proper analysis. Data analysis aids in the discovery of important nuances and leads to a positive outcome. Cybercrime is now a factor in all projects, as part of Malaysia's National Policy on Industry 4.0, which aims to improve the country's industrial capacity by enacting appropriate legislation to combat the use of ICTs for illegal purposes. Assuming that the cybercrime data is thoroughly investigated, the outcome might be quickly concluded, allowing better judgments to be made about combating cybercriminals through appropriate laws. Cybercrime is sometimes confused with a presentation that focuses solely on computers and the internet. However, not all cybercrime is limited to computers and the internet; for example, the instance of Joseph Marie

Jacquard and another common model would be dumpster diving , which is a tactic for recovering data that might be used to launch an attack on a computer network. Their presentation includes not just scanning the trash for valuables, but also getting access and a secret key written on scribbled notes (Lew, 2020).

Vizom is a popular video conferencing programme that is now important to companies and social life as a result of the coronavirus outbreak (Brewer, 2021). The danger with such attacks is that they can eventually lead to a cascade breakdown of interbank finance, perhaps sparking a bigger systemic liquidity crisis. In all of these circumstances, the companies' activities are so linked with those of other organisations in their respective countries that their collapse will certainly cause those other or connected businesses to fail as well. As a result, protecting such infrastructures, also known as key information infrastructures, is considered a national security concern.

Background of the study

Cyber-attacks are frequently in the news, posing a security risk to governments, sectors, and enterprises. Things might grow even worse with society's dependency on technology and the emergence of the internet of things. As seen by the devastating malware they employ to target enterprises, cyber thieves are becoming more intelligent and sophisticated.

This paper focuses on the current tend challenges of data analytic on cybersecurity in Malaysia and Malaysia is chosen to be the country for this research due to its strategic economic geographical location and Malaysia has been classified among the top ten nations with a strong commitment to cybersecurity in the International Telecommunications Union's Global Cybersecurity Index 2020 study (ITU). Malaysia faces many challenges in defending its cybersecurity domain. The information was gathered through interviews with experts in the field of cybersecurity. The findings indicated that in order to incorporate a cybersecurity aspect in the organisation, awareness and funding are critical. Due to the Prime Minister's digital economy blueprint, YAB Tan Sri Dato' Haji Mahiaddin container Haji Mohd, Yassin in 2021, a substantial increase in cyberisation would be 81 percent of Malaysians are now dynamic via web-based media in 2020, and 90 percent of government is now online (Mok, 2021). Simultaneously, concerns about cyber security approaches on advancement toward administrative arrangements command and updating outdated legislation are needed to provide robustness in combating cyber-attacks as Malaysia's cyberization progresses.

Literature Review

Industry 4.0 offers great benefits to businesses in terms of long-term viability. Internet of things, big data, supply chain, cloud computing, horizontal and vertical integration, autonomous robot, addictive manufacturing, cyber security, simulation, and augmented reality are the nine pillars in total. However, cyber security is the most significant problem in this digitalization era. The privacy and security of data will always be top security priorities for every firm.

All individuals, professionals, legislators, and, more broadly, all decision makers are concerned about cybersecurity. It has also become a big problem for societies that must protect itself against cyber-attacks using both preventative and reactive methods, which include a lot of monitoring, while still preserving their independence and avoiding widespread surveillance. Computer security, often known as cyber security or IT security, is the safeguarding of computer systems against harm to their hardware, software, or information, as well as disruption or misdirection of services they offer (Roca , 2019). Data integrity is a challenge in cyber security management. Due to the vast amount of information and data, securing data integrity in an IoT context has proven to be rather difficult. Data from many sources has a wide range of ideas and forms, making it challenging for analysts to combine it. Furthermore, a lack of monitoring and security against unauthorised modifications or alteration will result in undesirable data alterations. During peak hours, when enterprises may lack the internal competence and systems to manage and safeguard data, malicious data searchers are continually seeking for new methods to steal it (Campos et al., 2016).

Cybersecurity Data Analytic

The ultimate objective of cybersecurity data science is to use security data to make data-driven intelligent decisions for smart cybersecurity solutions. Cybersecurity data represents a partial paradigm change away from

old well-known security solutions like firewalls, user authentication and access control, encryption systems, and so on, which may or may not be successful in today's cyber business. The issues are that these are often handled statically by a few competent security analysts, with ad-hoc data management.

However, as the frequency of cybersecurity events in the various forms indicated above continues to rise, traditional solutions have proven ineffective in managing such cyber dangers. As a result, a large number of complex assaults are developed and disseminated swiftly throughout the Internet. Although several researchers use various data analysis and learning techniques to build cybersecurity models, as summarised in the section "Framework model in cybersecurity," a comprehensive security model based on the effective discovery of security insights and latest security patterns may be more useful. To overcome this problem, we need to create more flexible and efficient security systems that can respond to attacks and change security rules in a timely manner to mitigate them intelligently.

Table 1. Statistics on types of cybercrime in Malaysia 2022

	January	February	March	April	May	June	July	August	September	October	November	December	Total
Spam	8	5	6	15	0	0	0	0	0	0	0	0	34
Intrusion Attemp	15	12	4	6	0	0	0	0	0	0	0	0	37
Vulnerabilities Report	6	3	3	4	0	0	0	0	0	0	0	0	16
Malicious Codes	62	68	174	103	0	0	0	0	0	0	0	0	407
Content Related	2	0	0	2	0	0	0	0	0	0	0	0	4
Denial of Service	0	2	1	1	0	0	0	0	0	0	0	0	4
Intrusion	68	54	50	74	0	0	0	0	0	0	0	0	246
Fraud	431	423	388	396	0	0	0	0	0	0	0	0	1638
	592	567	626	601	0	0	0	0	0	0	0	0	2386

Table 1, data indicates the statistic on types of cybercrimes in Malaysia 2022. In order to analyse the data coherently to reflect the accuracy, it is necessary to evaluate a large quantity of important cybersecurity data collected from many sources, such as network and system sources, and to identify insights or correct security policies in an automated way with little human interaction. Analyzing cybersecurity data and developing the necessary tools and methods to effectively guard against cybersecurity events entails more than a basic set of functional requirements and understanding of risks, threats, and vulnerabilities.

Proposed framework to safeguard data analytic for cybersecurity

As previously stated, cybersecurity data science is data-driven, employs machine learning techniques, attempts to quantify cyber risks, employs inferential techniques to analyse behavioural patterns, focuses on generating security response alerts, and ultimately seeks to optimise cybersecurity operations. As a result, the researchers briefly explain a layered data processing architecture that can be utilised to extract security insights from raw data and develop smart cybersecurity systems, such as dynamic policy rule-based access control or intrusion detection and prevention systems.

Collecting relevant cybersecurity data is a critical stage that serves as a link between cyber infrastructure security issues and data-driven solution processes in this methodology. As a result, the question is how to gather relevant and unique requirements data in order to construct data-driven security models. A strict framework, such as proposed policies and legislations, should play an essential role in safeguarding pure cybersecurity data for analysis.

This layer in this framework is responsible for finalising the resulting security model by including new intelligence as needed. This might be accomplished by additional processing in numerous modules, such as recency mining and security model updating, which is responsible for keeping the security model up-to-date for improved performance by extracting the most recent data-driven security patterns.

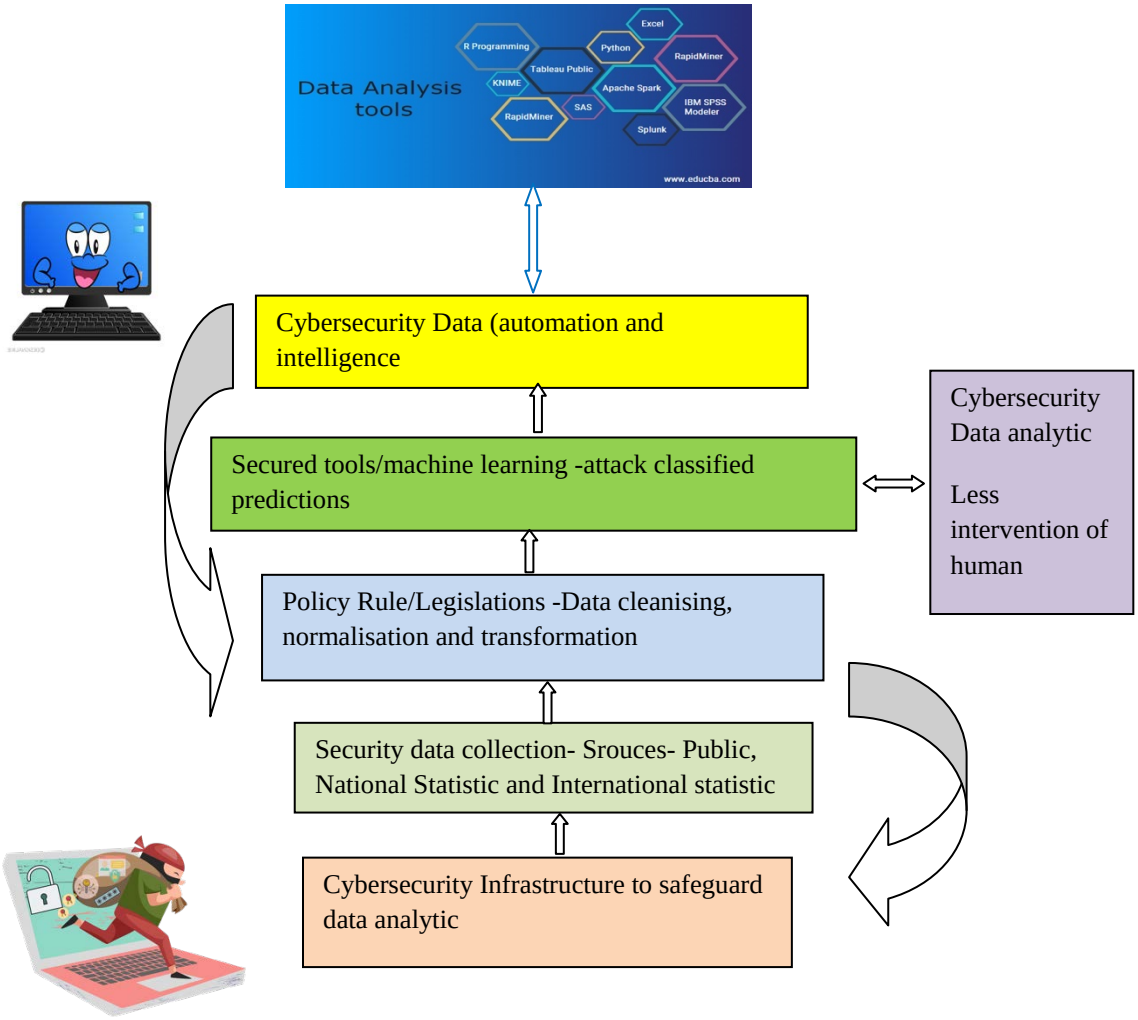

Figure 1. Cybersecurity layered data processing architecture framework

Results and Discussion

Data from computer networks, telecommunication networks, banking, healthcare, social media networks, bioinformatics, E-Commerce, surveillance, and other sources are some of the most common sources of big data transactions. The absence of security software that can be upgraded for protection is the next issue (Yaaqob et al., 2017). Due to a scarcity of equipment, tools, and systems, this is the case. An organization's software upgradeability is also expensive. On the one hand, most businesses are unable to organise unstructured data (Campos et al., 2016).

From the proposed framework in Fig.1, it is predicted that with this high level proposed data cleaning , normalisation and a comprehensive policy and legislation in place, the cybersecurity of Malaysia will be fully protected and moreover data-driven intelligent decision making in smart cybersecurity systems and services is what cybersecurity data science is all about.

Conclusion

Finally, the researchers have emphasised the current state of the art difficulties confronting the cybersecurity area in the face of data analytics. Traditional security solutions, employing traditional tools and methodologies, are no longer capable of embracing real-time large data network streams. Security analytics, or the use of structured data analytics to derive actionable knowledge and insights from streams in real time while adhering to governing rules, has been demonstrated by researchers to be a growing necessity for cybersecurity installations. Although the present usage of analytical solutions is far from revolutionary (as demonstrated by this Teradata research from 2013), awareness of adoption is gradually growing.

Recommendations

The discussion of this research was centred on two objectives: (1) analysing Malaysia's cyber security difficulties, and (2) proposing a holistic cybersecurity data analysis methodology for Malaysia to address cyber security challenges. Although Malaysia has cyberlaws in place to combat cybersecurity breaches, such as the Computer Crimes Act 1997, the Communications and Multimedia Act 1998, the Penal Code,the National Cyber Security Agency (NACSA) and the Malaysia CyberSecurity Strategy 2020-2024 , the topic of cybercrime and cyber security is still very popular, and free data sets for analysis in this field are still scarce. Data analysis for cybersecurity will be more accurate to forecast and prevent cybercrime in Malaysia if more data in this industry becomes available and extracted with minimal human interaction.

Scientific Ethics Declaration

The authors declare that the scientific ethical and legal responsibility of this article published in EPSTEM journal belongs to the authors.

Acknowledgements or Notes

This article was presented as an oral presentation at the International Conference on Basic Sciences, Engineering and Technology (www.icbaset.net) conference held in Istanbul/Turkey on August 25-28, 2022.

*This research is funded by the Malaysian Ministry of Education (MOE) through the Fundamental Research Grant Scheme (FRGS) FRGS/1/2019/SSI10/MMU/03/15. The authors alone are responsible for the views expressed in this article, which does not necessarily represent the views, decisions, or policies of MOE or the institutions with which the authors are affiliated. The funder had no role in study design, data collection and analysis, or preparation of the manuscript.

References

Brewer, R. (2015). Cyber threats: reducing the time to detection and response. *Network Security, 5*, pp.5-8.

Communications and Multimedia Act (1998). *National Cyber Security Agency (NACSA)*. https://www.nacsa.gov.my/

Malaysia CyberSecurity Strategy 2020-2024 Compressed.pdf https://asset.mkn.gov.my/web/wp-content/uploads/sites/3/2019/08/MalaysiaCyberSecurityStrategy2020-2024Compressed.pdf

Global Cybersecurity Index (2020). https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

Campos, J., Sharma, P., Jantunen, E., Baglee, D., & Fumagalli, L. (2016). The challenges of cybersecurity frameworks to protect data required for the development of advanced maintenance. *Procedia Cirp, 47*, 222-227.

Lew, H. (2020, January 29). *Why malaysia should amend its cyber security laws*. Asia Law Portal

Mok, O. (2021, February 19). *MyDIGITAL and Malaysia digital economy blueprint: how we can achieve 100pc internet access.* Malaysia | Malay Mail

Roca, S. K.-L.-D.-V. (2019). Cybersecurity current challenges and Inria's research directions. *Le Chesnay Cedex, France: Inria*

Teradata and Ponemon Institute (2013). Big data analytics in cyber defense, February. http://www.ponemon.org/local/upload/file/Big_Data_Analytics_in_Cyb er_Defense_V12.pdf

Yaqoob, I., Ahmed, E., ur Rehman, M. H., Ahmed, A. I. A., Al-garadi, M. A., Imran, M., & Guizani, M. (2017). The rise of ransomware and emerging security challenges in the Internet of Things. *Computer Networks, 129*, 444-458.

Author Information

Shereen Khan
Multimedia University
Persiaran Multimedia , Cyberjaya 63100, Selangor, Malaysia
Contact e-mail:*shereen.khan@mmu.edu.my*

Tan Swee Leng Olivia
Multimedia University
Jalan Ayer Keroh Lama, 75450 Bukit Beruang, Melaka, Malaysia

Nasreen Khan
Multimedia University, Malaysia
Persiaran Multimedia , Cyberjaya 63100, Selangor, Malaysia

Ng Kok Why
Multimedia University, Malaysia
Persiaran Multimedia , Cyberjaya 63100, Selangor, Malaysia

Swee Wei Tan
Multimedia University
Persiaran Multimedia , Cyberjaya 63100, Selangor, Malaysia

To cite this article:

Khan, S., Olivia, T.S.L., Khan, N., Why, N.K. & Tan, S. W. (2022). Data analytic for cyber security: a review of current framework solutions, challenges and trends. *The Eurasia Proceedings of Science, Technology, Engineering & Mathematics (EPSTEM), 18,* 1-6.