Leveraging the Benefits of Big Data with Fast Data for Effective and Efficient Cybersecurity Analytics Systems: A Robust Optimisation Approach

Paresh Rathod[1] and Timo Hämäläinen[2]
[1]Laurea University of Applied Sciences, Espoo, Finland
[2]University of Jyväskylä, Finland
paresh.rathod@laurea.fi
timo.t.hamalainen@jyu.fi
DOI: 10.34190/ICCWS.20.034

Abstract: In recent times, major cybersecurity breaches and cyber fraud within the public and private sectors are making international headlines. Majority of organisations are facing cybersecurity adversity and advanced threats. On the one hand, we have asynchronous cybersecurity practices, many standards and frameworks to consider while on the other hand, we have to deal and secure our organisations against cyber-criminals, organised hacktivists, insider threats, hackers and nation-states with malafide intentions. The Center for Cyber Safety and Education's Global Information Security Workforce Study (GISWS) confirms that globally we are not only loosing but also backpedalling against threats and risks at cyberspace. How do national-protection actors and organisations conduct and practice their cybersecurity to protect against dramatic attack surfaces? Most importantly, how do they allocate limited cybersecurity resources in defence? Most organisations advice to adopt systematic approaches using standards, framework, audits and best practices. However, the current security technologies, policies and processes are lacking robust cybersecurity capabilities and a mechanism to solve advanced cyber threats and risks. In this paper, we are proposing a novel solution to detect and protect against advanced cybersecurity challenges by leveraging the benefits of big data security intelligence with fast data technologies. The paper is presenting a technology-independent reference model utilising a robust optimisation approach for the cybersecurity analytic systems. This study is utilising state-of-the-art and cutting-edge reference model and solution that enables cyber secure internet and digital technologies usage along with underlying data network and information systems in the multi-organisational environment. The underlying solution enables interoperability and flawless message and information exchanges within national protection actors. The study concludes with the proof-of-concept in the cyber secure decentralised multipurpose communications network.

Keywords: advanced cyber threats, cybersecurity, cybersecurity analytic systems, big data, fast data, big data analytics

1. Introduction

In recent years, the unforeseen challenges for cybersecurity emerged dramatically. On the one hand, we have asynchronous cybersecurity practices, many standards and frameworks to cope with while on the other hand, dealing with the broad threat-agent vectors including nation-states, online criminals, organised hacktivists, insider threats and hackers with malafide intentions. The Center for Cyber Safety and Education's Global Information Security Workforce Study (GISWS) conducted in the year 2017 confirms that globally, we are not only loosing but also backpedalling against threats and risks at cyberspace. There is a gap and requires a better cybersecurity solution. This paper addresses these gaps and proposing a novel solution for cybersecurity by leveraging the benefits of big data intelligence with fast data technologies. Chen et al. (2017) and Haldorai and Arulmurugan (2018) argued that big data analytics showed strength for targeted analysis and prediction of security incidents and risks. Haldorai and Ramu (2018), Rajamäki and Simola (2019) also presented utilising the fast data on top of the big data layer can dramatically improve the performance of data mining and analysis.

This paper is providing proof-of-concept by combining and leveraging benefits of both technologies to strengthen the cybersecurity analytic systems (CAS) for decentralised communications within critical information infrastructure protection (CIIP). The research work is contributing towards the European Unions (EU) digital agenda, where this study is ultimately aiming to provide solutions for cyber-secure digitalisation and decentralised communications.

The previous research work of Rajamäki, Rathod and Holmström (2013) and Rajamäki and Simola (2019) addressed not only the technical challenges of security and interoperability but also the strategy to build a redundant critical governmental communication system for a multi-organizational environment; enabling external users to collaborate towards keeping the intrinsic and vital security mechanisms of such networks.

The paper is structured and divided into six sections, starting with an introduction to the research study. The next section describes the background and current state of research studies. Further, this section also formulates the research gap and problems. The third section is covering the concept of research and development process. Section four is presenting and justifying research method used in this study. Further, we are presenting a conceptual solution and model in the fourth section. Finally, we are exploring other possibilities, discussion and future direction in subsequent sections.

2. Background and research problems

The Internet and the broader concept of 'cyberspace' have, over the last ten years, providing businesses with new opportunities for competitive advantage and a new vector for further economic growth. The cutting-edge technologies have greatly enhanced the smooth functioning of government, military and industrial organisations and their information and communications systems. Many times, the critical infrastructure (CI), also known as 'systems of systems', it consists of collections of information systems and networks. The critical infrastructure directly intervened with the economy and social well-being of a secure society within member states in EU. The critical information infrastructure (CII) consists of ICT systems that are critical infrastructure themselves and essential for the operation of critical infrastructure including telecommunications, computer hardware and software, internet, satellites and underlying technology backbone.

On the one hand, we are leveraging the benefits of the digital world. At the same time concerns about the security of cyberspace have also grown exponentially, especially within critical infrastructure domains. The criminals are continuously looking to exploit this new environment for their own economic, political and personal benefits. Increasingly, a priority concern associated with the potentially sensitive, classified and personal information that is stored and processed by national protection actors and organisations. Carcary, Doherty and Conway (2019) and many researchers argued that one of the key reasons for rapidly increasing breaches denoted to "attack surface" in addition to increasing vulnerabilities, number of internet users, and number of users accessing online resources. Generally, the attack surface includes a set of ways in which an adversary can attack the system. How do organisations conduct and practice their cybersecurity to protect against dramatic attack surfaces? Most importantly, how do they allocate limited cybersecurity resources in defence? This situation is demanding more sophisticated and smooth security solutions that can deal with unforeseen challenges. Many research argued that cybersecurity analytic systems could provide robust security with smooth data transactions including the work of Hafsa and Jemili (2019), Ullah and Babar (2019).

This research study is investigating the current state of the big data analytics with cutting-edge technologies of fast data within cybersecurity perimeters. According to many research sources, including commercial Goldman Sachs Global Investment- there are few key technology trends including increasing economic bandwidth, processing power, smartphones, wireless coverage, big data and security technologies. Therefore, it is vital to understand the current state-of-the-art (SOTA) and trends of cutting-edge technologies within the cybersecurity domain. The following subsections are presenting a few key findings.

2.1 Current digital connectivity snapshot and evolving cybersecurity challanges

In the past, a report estimated that around 8.7 billion computers connected to the internet in the year 2012. Camhi, J. (2015) presented comparable statistics; this report estimates the existence of around 20-24 billion connected devices. Current trends towards the IoT (internet of things) and the continued proliferation of mobile devices means that the scale and diversity of connected devices set to continue to grow exponentially. Many research data including Huskaj (2019) predicts the number of connected and networked devices will increase up to 75 billion by 2020 and 100 billion by 2025. The ongoing research study helps to visualise the growth of global digitalisation as shown below; see Figure 1.

Besides, the users are switching from conventional analogue to digital systems. The digitalisation continues in all vertical sectors, including utilities to public safety. Even critical communication is witnessing a significant digital transformation. On the one hand, there is a rapidly growing digital connectivity across the globe. These trends demand a high level of information and cybersecurity to ensure trust and confidence within national protection actors and users (Alaba et al, 2017). On the other hand, the cost of cybercrime and the scale and frequency of attacks continues to increase within civilian and national protection actors' information and communications technologies (ICT). Therefore, it is vital to find economically viable solutions.

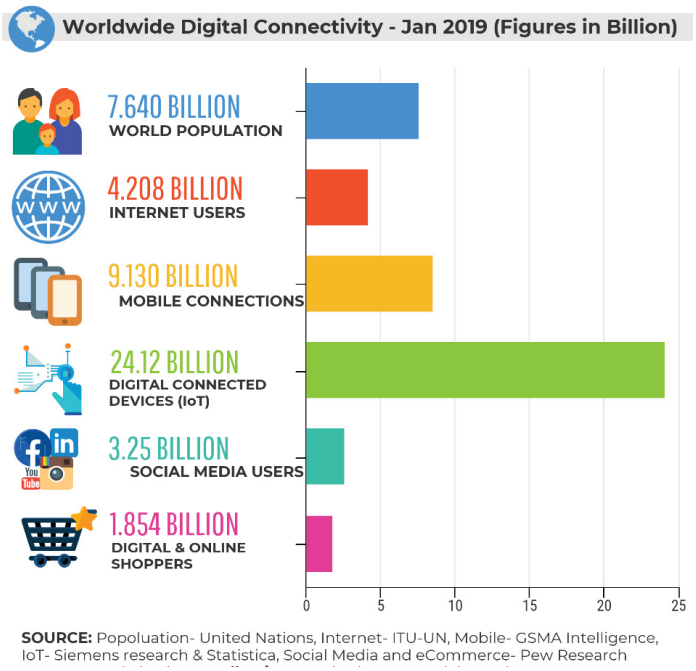
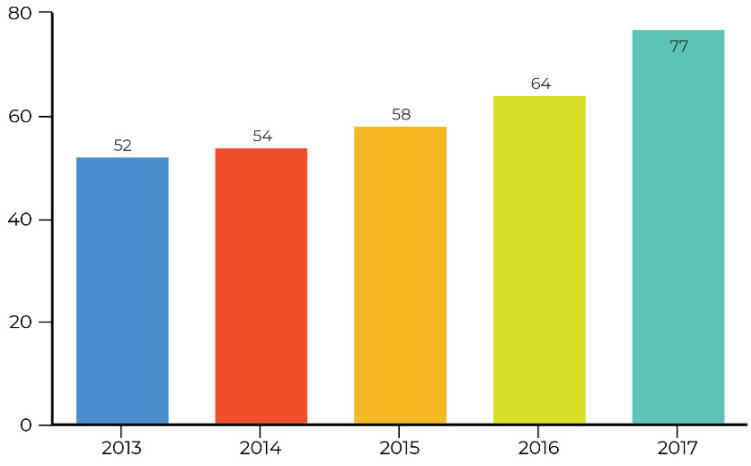


Figure 1: The Worldwide Digital Connectivity in Numbers (data presented by authors, 2019)

2.2 Cyber Threats and Cybercrime leads to Economic Catastrophes

Recently, cybersecurity threats and risks are rapidly increasing than ever before. Bengtsson Borg and Rhinard, M. (2018) present the threats and risks are mainly on people-centred, process-centred and technology-centred issues. The computer technologies are becoming ubiquitous, interdependent and complex, especially in critical infrastructures and its communication. Therefore, any disruption in one component can lead to the failure of the whole system.

On the other hand, the intensity of cyber threats and risks are evident in recent times. The steady increase in cyber-attacks with high number and complexity pauses a massive challenge to national protection actors and organisations. Mainly, the damage caused by cyber-aggressors including cyber-terrorists, cyber-spies, cyber-thieves, cyber-warriors and cyber-hacktivists. Besides, script kiddies, web defacers, hackers, pirates and phone-phreakers are also carrying out attacks. The most critical cybersecurity challenge faced by critical infrastructure is advanced-persistent threats (APTs). The paper is also addressing the challenges faced by such severe cyber threats and risks on critical infrastructure communications.



Consolidated view: Average n=252 companies in last 5 years, cost expressed in USD.
SOURCE: Ponemon Institute, IBM and Accenture

Figure 2: Average Highest Cybercrime Costs in USD Million (data presented by authors, 2019)

The Cyber Security Breaches Survey conducted by Finnerty et al. (2018) reveals more than 40% of businesses faced cybersecurity attacks and breaches within last year. The official data released by the UK government under Cyber Security Breaches Survey 2018. The recent study by Ponemon Institute showed that on average annual losses to companies that suffered a successful cyber attack globally was the US $3.86 million. The following figure demonstrates the highest cost of cybercrime within studied companies (average of 252 companies every year) in the last five years; see Figure 2. The shocking facts came out of many independent studies and reports that the data breaches, cyber-attacks and cyber crimes are costing close to the US $600 billion globally; it is demonstrating the state of 'Epidemic' on the digital world. The lack of comprehensive and holistic cybersecurity solutions can only add another quadrupling or more costs in coming years. Such an epidemic needs a great sense of urgent remedy and solution (Eling and Wirfs, 2019). This study is consolidating cybersecurity with big data analytics using fast data technology, as explained in subsequent sections.

3. The gaps in the current state of the art (SOTA) and research questions

The Center for Cyber Safety and Education's Global Information Security Workforce Study (GISWS) confirmed that globally, we are not only loosing but also backpedalling against threats and risks at cyberspace. ENISA and Brookson et al. (2015) research study confirmed that there are gaps in existing systematic approaches of cybersecurity. The study found gaps in the following five categories: talent, management, budget, technology and parity gaps. Besides, many research studies also claiming the lack of a holistic solution pausing one of the biggest challenges for cybersecurity. The research studies also found that the balance, appropriate and intelligent solution is enhancing the cybersecurity significantly.

This paper is focusing on addressing technology, parity gaps and appropriate intelligent solution using big data intelligence with fast data technologies for cybersecurity analytics systems. The technology gaps, mainly the rapid growth of cyber threats are not addressed quickly with the deployment of security technologies. Over the past years, various research proved that intrusion detection and prevention is undecidable and bound to produce errors (Kabir and Hartmann, 2018). The current security solutions are effective within known threat and risk vectors but showing weaknesses and shortcomings for unknown cybersecurity risks. Kabir and Hartmann (2018) argued that integration and scalabilities are also the most significant challenges due to the strong influence of vendor-specific static security solutions. With rapidly increasing networks and large datasets, existing attempts for monitoring network, finding sophisticated threats and providing security solutions not possible. These challenges become a 'big data issue', this paper is addresses following key research question: How can big data analytics utilised with fast data for a technology-independent cybersecurity reference model with a robust optimisation approach for the cybersecurity analytic systems? The paper is addressing shortcomings and challenges by proposing novel cybersecurity analytic systems model utilising big data analytics and intelligence with fast data technologies.

4. The research approach and method

This research study is aiming to develop a systematic novel model using inductive reasoning scientific method considering the analytic reasoning process. The inductive reasoning is starting with the observation of phenomena, forming patterns and the tentative hypothesis that results in novel solution and theory (McAbee et al., 2017). The method is strongly base on providing a solution.

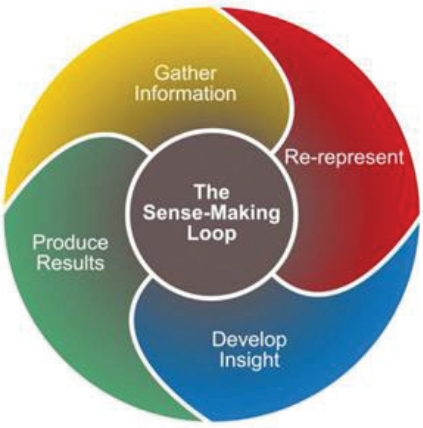


Figure 3: The Analytical Reasoning Process (Thomas, 2005)

The analytic reasoning method draws the premises from unknown to known with an iterative process that develops confidence in achieved solutions and hence ensures the trust. The approach is a structured, iterative process based on inductive reasoning; see Figure 3. In this method, the goal of the analyst is to reach a judgement about an issue or problem. The outcome of analyses presents the tangible results in the form of a novel model or product. The process starts with the planning of proving solutions to given issues. The planning phase includes resource usage and timeline plan. The second step in the process includes gathering and familiarising with available information on top of the already gathered information. Next, the analyst hypotheses and outlines multiple candidates with explanations. This step represented in developed insight steps in the process; see Figure 3. Indeed, analyst aiming to reach a judgement by evaluating alternative explanations. The whole process allows expanding and broadening understanding of the analyst's previous thinking. The analysis process ends with the final step represented in Figure 3. (i.e., produce a result). The final step allows an analyst to summarise the judgement with the creation of reports, documents, models, services or products.

In a nutshell, the inductive reasoning method starts with the specific observations and measures that allow detecting patterns and regularities and resulting in formulating some tentative hypotheses to explore. Finally, the explorations of hypothesis end with broader generalisations, developing conclusions or drawing theories.

This scientific method is an ongoing and iterative process. Analytical reasoning is an iterative and highly collaborative methodology-people, process and technology synchronously scale to support cybersecurity reasoning, assessment and actions. Further, cyber-secure critical infrastructure communications model will be developed for smooth operations by national protection actors as a proof-of-concept. Finally, the outcomes can be disseminated to ensure trust within the European digital single market.

4.1 Gathering Information to Develop Insights

This study started with specific observations, systematic literature reviews and measures exploring and searching digital databases including ACM, Emerald Insight, Google Scholar (for a variety of literature), IEEE Xplore, ScienceDirect and Wiley. Our systematic literature review followed the steps starting from research target and questions, literature review strategy, setting targeted criteria, identifying relevant studies, analysing data and synthesising processes. Our study is developing insights and producing results that represent an effective and efficient novel model for big data with fast data technology for cybersecurity analytic systems. To reach our target, we have identified the following research questions: (1) Which are the essential components for effective and efficient cyber-secure analytic systems? We focused on reviewing, deep-analysing and measuring highly relevant studies on big data analytics, fast data and its usage in effective and efficient cybersecurity analytic systems and relevant architectures. Our study identified measurable attributes that provide effective and efficient analytics for cybersecurity systems. (2) How does the big data analytics process with fast data technologies enhancing the robust cybersecurity analytics systems? The cybersecurity analytic systems are aiming for the optimised novel solution utilising existing best practices and solutions.

The output of studied literature and selections presented in this paper, as the scope of this paper, is to present novel solutions using the big data with fast data for cybersecurity analytic systems and its architecture. The scope of paper restraining to present the complete and deep analysis of the data. However, the paper is presenting the summary of in-depth analysis using qualitative data analysis that includes the step-1 to 3 from analytical reasoning process (refer Figure 3 and Table 1) starting from gathering information, re-representing and developing insights. The first step is gathering information, including keywords for titles, abstracts and full text for learning state-of-the-art (SOTA). The next step the finding re-representing by identifying most relevant work beyond state-of-the-art (BSOTA). The final step is developing insights by implementing a sense-making loop and extracting new insights.

4.2 Produce Results

The outcome of deep analysis steps resulted in quantifying quality attributes of cybersecurity analytic systems as listed here alphabetically below; see Figure 4.

Table 1: Analytic reasoning process with collected data

From SOTA to Develop New Insight			
Database Source	**Gathering information**	**Re-represent**	**Develop insight**
ACM	219	24	68
Emerald Insight	85	9	
Google Scholar	98	11	
IEEE Xplore	175	12	
Science Direct	95	8	
Wiley Digital Database	35	4	
Total:	707	68	68

The list of cybersecurity analytic systems' quality attributes and components are the result of our extensive literature review and statistical analysis implementing step-1 to 3 of the analytical reasoning process (refer to Figure 3 and Table 1). Our study found significant correlations between the above findings and proven science of the software quality attributes presented by Madan et al. (2002) and Bachmann et al (2005). We are not presenting the complete analysis here; mainly the scope of the paper is to present a novel model avoiding complex detailing. However, the list of the quality attributes of cybersecurity analytic systems presented in Figure 4 that includes accuracy, adaptability, efficiency, generalisation, interoperability, learnability, modifiability, performance, privacy robust, reliability, resilience, robustness, safety, scalability, security, Stealthiness and usability. Evans et al. (2019) presented the quality attributes that can be adopted with all three cybersecurity analytic systems, including host-based, network-based or hybrid.

The robust cybersecurity analytic systems offer versatile application domains including alerting, intrusion detection system, several threats detection, forensic analysis and defending unknown threats by adopting quality attributes (McAbee et al., 2017).

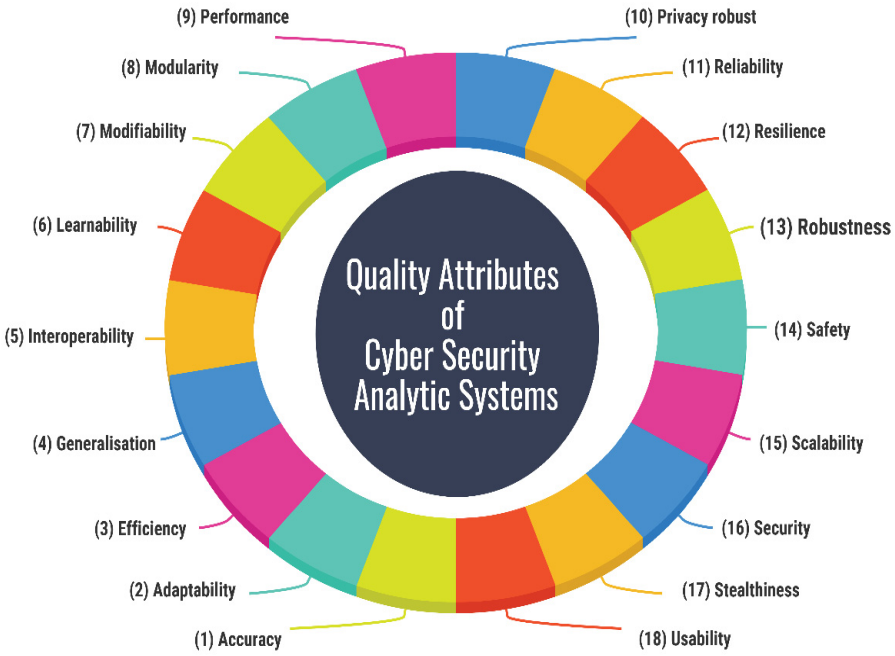


Figure 4: Quality Attributes of Cybersecurity Analytic Systems (presented by authors, 2019)

The study outcomes are answering the first research question that seeks the essential components for effective and efficient cyber-secure analytic systems. Next, we are using these quality attributes in conjunction with big data analytics and fast data technology for effective and efficient cybersecurity analytic systems — further, the results and outcomes been implemented as a proof-of-concept within critical information infrastructure as a part of the on-going sense-making loop in the analytical reasoning process.

5. A novel model – cybersecurity analytic systems utilising the big data intelligence

The cybersecurity challenges arose along the ubiquitous and widespread use of computers and the internet. Ren et al. (2019) state that technological development allows realising the big data intelligence using data analytics including data mining and predictive analytics. This paper is presenting said model and solution in following subsections.

5.1 Big Data and Data Analytics

The big data can be simply described as a set of large and continuously growing data with the characteristics of volume, velocity, variety, complexity and value.

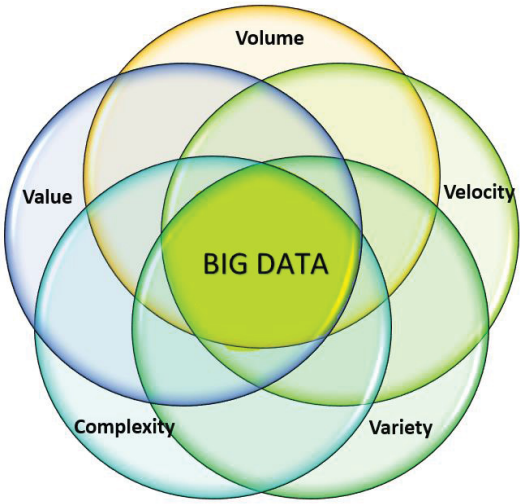


Figure 5: Extended Model of the Big Data (presented by authors, 2019)

Usually, the big data are coming from various sources including structured, semi-structured and unstructured large and massive volumes of data that cannot be managed by traditional technology including relational database management system. It is evident- what was considered as the Big Data before few years might not be considered as the Big Data now. Equally, today's Big Data might not be considered as the Big Data a few years from now (Mtsweni and Mutemwa, 2019). The big data characteristics can be defined as below:

- Volume: The stored quantity of data.
- Velocity: The data transaction speed.
- Variety: Different forms and types of data.
- Complexity: The big data with difficulties of managing interconnections and linkages.
- Value: Provides specific usefulness to an organisation.

Katal, Wazid and Goudar (2013) argued- there is an ongoing disagreement about the definition of Big Data. The authors are arguing and presenting the following figure as a modern representation of Big Data in addition to the 3 Vs; see Figure 5. Authors have observed the phenomenon of continuous evaluation of complex data and the definite need for value creation of big data for organisations.

5.2 Big data analytics and fast data processes in cybersecurity

On the one hand, Ishikiriyama and Gomes (2019) argue that massive and ever-increasing data collected for cybersecurity; including network and system logs, user information and authentication data, network packet traces, software and web applications, and many more. On the other hand, Bendovschi (2015) presents that the attack patterns are unexpected, actively changing the behaviours and frequently bringing adversaries. The aim is utilising big data analytics in cybersecurity to provide actionable insights to resolve any security challenges. These developments are demanding novel tools and techniques utilising interaction between big data analytics and cybersecurity (Babiceanu and Seker, 2016). The traditional data processing and analytics technique cannot handle unstructured and non-relational databases. Ishikiriyama and Gomes (2019) also presented that the cutting-edge and emerging big data analytics technology helps to collect, store, process, analyse and visualise simplified outcomes of massive unstructured and non-relational datasets. It uses advanced data processing and analytic techniques including data mining, machine learning, text analytics,

clustering, predictive analytics, natural language processing and other. The big data analytics helps to find and learn hidden patterns, market trends, unknown customer needs, and many more unforeseen insights. The large body of research confirms that big data analytics is one of the most useful tools to improve business processes and performance. The big data provides promising advantages supporting unstructured data, distributed storage and fast data processing. These insights can be useful together with risk management processes to minimise and mitigate cyber risks, enhances awareness and incident response with more economical viable cybersecurity solutions. We are proposing optimised and simplified model for big data cybersecurity analytics processes depicted in subsequent sections.

The current scale of big datasets put limits to process on data as it arrives (Wampler, 2018). The quick storage and processing of data demanded novel solution and fast data technology unlocks the value of rapid processing and responding for big data analytics. The fast data technology enables real-time and concurrent analysis, deeper insights and appropriate responses. The big data analytics utilising with fast data provides increased throughput, high performance, scalabilities and real-time intelligence beyond stream analytics (Velásquez, Munoz-Arcentales and Salvachúa, 2018).

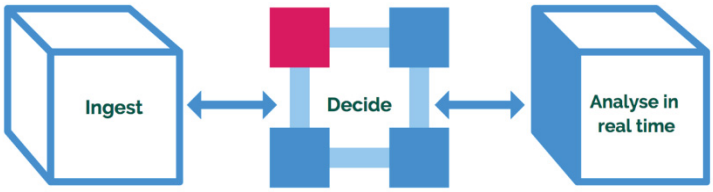


Figure 6: Fast data process architecture (presented by authors, 2019)

The fast data technology enables big data analytics for better cybersecurity solutions, due to its capabilities for rapid updates. The combination of fast and big data is more effective within applications that are running with low latency and high input-output. The novel analytic system aims to collects, processes and analyses structured or unstructured data from millions of connected computers and devices, and provides smart insights to take required actions. The fast data processing visualised in the following model; see Figure 6. The fast data technology is highly effective while processing big data streams. The fast data follows a three-step process: ingest, decide and analyse in real-time. In a nutshell, the process is straightforward and highly effective where ingest takes millions of events per second, then makes data-driven decisions and finally, enables smart decision and visibility for working situation.

6. The Novel Model

This section is presenting a novel model combining the benefits of big data and fast data technologies by filling the gap in the state-of-the-art where cybersecurity analytic systems provide the benefits of the quality attributes presented in section 3.2. The following figure presents the novel architecture; see Figure 7. The benefits of big data analytics increase when it gains deeper insights and enables rapid solutions as demonstrated in the novel model.

The model presented from left-to-right as explained here: (1) Data sources represented collectively with structured, semi-structured, unstructured, mobility, streaming and other categories. In principle, they are categorised within mobility and structure of the data. Generally, mobility data can be moving or not moving. For example, streaming data are moving and need to be processed real-time (Wampler, 2018). On the one hand, structured data stored under traditional and strict model including relational databases. On the other hand, unstructured raw data have no data model. For example, images, web pages and content. Semi-structured remain in between these. For example, JSON or XML document data.

(2) Data extraction starts with the input of static data to the system process. These data can be temporarily stored or transferred in data storage. This component holds functionality of data extractions and stream-extraction and the data store of stream temp-data. (3) The fast data processing compresses data in real-time improves efficiency before transferring to load operation. This component holds the functionality of transfer and load, and data stores of raw data holding unprocessed data. (4) Data processing components hold the functionalities including stream processing, information extraction, and combining, replicating, experimenting

and cleaning — the data stores including enterprise data, sandbox, preparation data and stream data. The fast data processing improving the quality of raw data and prepared data. (5) Data analysis is one of the most important components that holds deep and stream analysis functionalities. The fast data processes extract new information efficiently for deep analytics. The data store includes analysis results, publish and subscribe, and stream analysis results. (6) Data loading and transformation component includes the functionalities of transformation, transfer and load while data stores include serving data. The fast data processes help data analysis securely transformed into serving data storage. (7) Fast data processes accurately perform with all quality attributes abstracts serving data towards interfacing and visualisation applications.

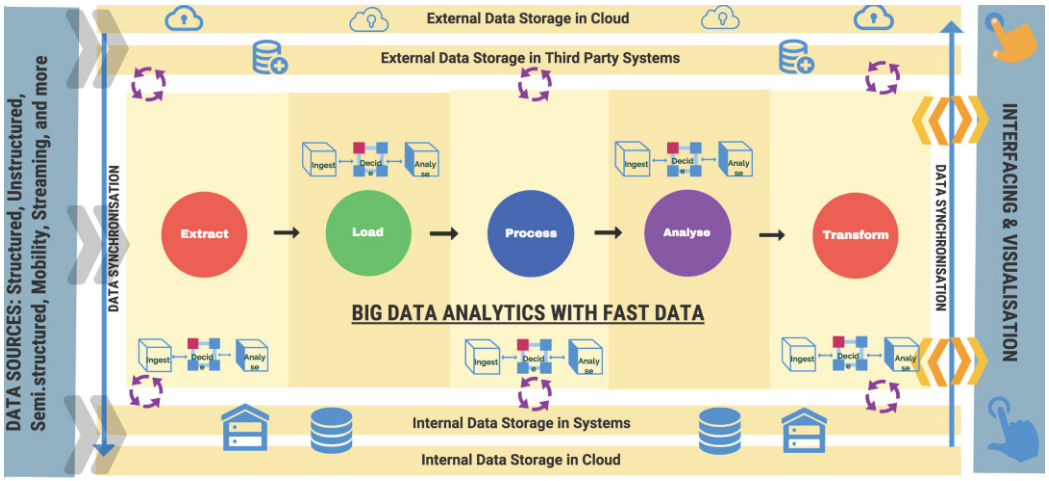


Figure 7: Novel Model of Cybersecurity Analytic Systems (presented by authors, 2019)

The online analytical processing (OLAP) queries helping to abstract the big data intelligence in the form of simple user interface dash-boarding application, visualisation and control functioning visualisation application, and end-user application, including mobile apps. These interfacing and visualisation component provide smart decision information, key performance index and information, and action steps for effective and efficient cybersecurity (Du et al., 2018, Bazarkina, 2019, Carrol, 2010). Our study suggests to utilising current solutions to expand cybersecurity analytic systems for a smart decision that consolidates security. For example, a layer of fast data within big data analytics enhances data processing effectiveness and efficiencies.

7. Proof of the concept

The previous research studies of Rajamäki, Rathod and Holmström (2013) and Rajamäki and Simola (2019) argued and presented decentralised fully redundant cyber-secure communication concept for critical information infrastructure (CII) and communication actors including government and national agencies. The authors argued, “The decentralised architecture concept is using the Distributed Systems intercommunication Protocol (DSiP). The concept is highly fault-tolerant in routine as well as crises operations. The software-based approach is independent of heterogeneous data communication technologies, IP networks and telecommunication operator services. The solution enables to build an effective and lasting cyber-secure data network for multi-organizational environment. Being a fully decentralized concept, networks of individual member organizations are virtually autonomous and hard to upset each other. That allows smooth message and information exchange to enable interoperability.”

These research results are still valid. However, many issues need a robust solution including accuracy, scalability, performance, reliability, and security. We are aiming to provide proof of concepts of our novel solution for critical information infrastructure and communications. We are proposing an extension to previous research finding to fill-the-gap emerged from new threat vectors, scalability and need of synchronous communications of national actors across EU nations

We are proposing more effective and efficient solution utilising cybersecurity analytic systems within decentralised multipurpose communications module for CII actors. The proof-of-concept connects the component of cybersecurity analytics systems with each node of DSiP router through hardware firewall to collect the data within decentralised communication systems and third-party cloud data sources to utilise the intelligence of big data with fast data technologies.

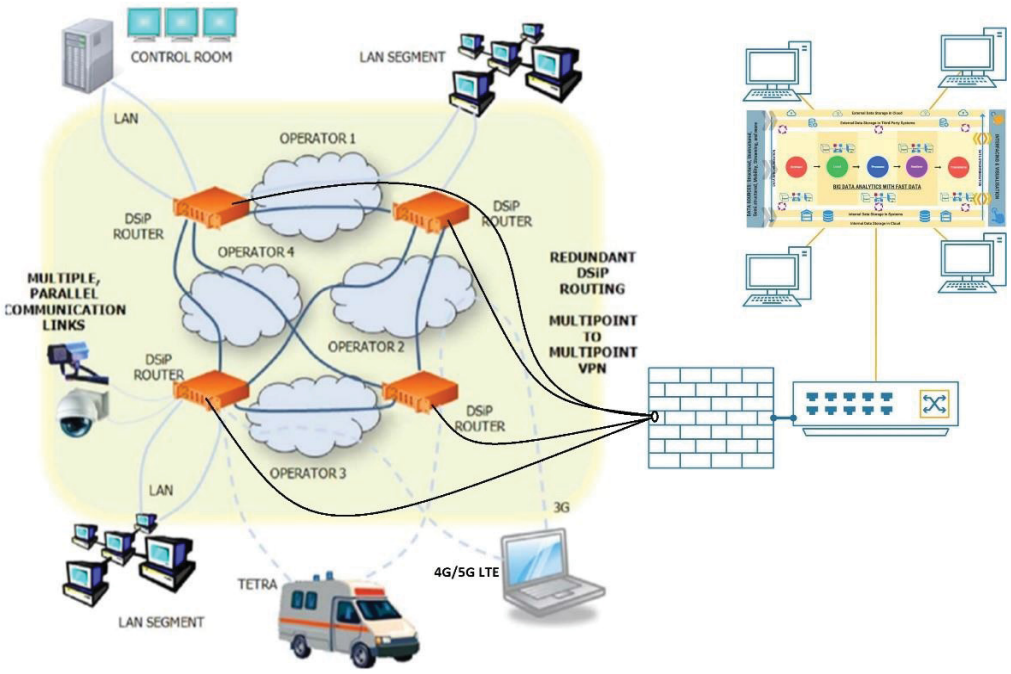


Figure 8: Cybersecurity analytic systems proof of concepts within critical information infrastructure (CII)

The previous research work manifested that DSiP based communication is robust and straightforward as it is a software protocol based solution where two elements are essential: DSiP routers and DSiP nodes. The proof-of-concept is connecting cybersecurity analytic systems router with the DSiP routers. The integrated system enhances secure communications with efficiency. This implementation is simple as it is an extension to existing decentralised systems. The existing system may include any legacy systems within technology eco-system; however, the mapping with cybersecurity analytic systems could not affect the previous complexity. Besides, this additional component optimises the security of decentralised communications and makes robust cyber-secure communications. Typically, DSiP-routers and Security Analytic Systems-routers are distributed in different physical locations within the routing network. This is adding addition flexibilities when it comes to decentralised distributed network and communications. The proof-of-concept demonstrated in above visual; see Figure 8.

8. Conclusion and future direction

The traditional cybersecurity solutions are struggling to provide robust and reliable security against revolving threats and cyber-attacks. The very notion is seeking effective and efficient cybersecurity mechanism and solutions. The advancement in technologies provide diverse possibilities, for example, emerging technologies including big data and fast data are used for business analytics that collects, stores, processes and visualize for smart and reliable decision-making. The big data trend is allowing cutting-edge analytical technologies to leverage the benefits in the various field for more robust solutions. As on now, cybersecurity becoming a big data challenge intervening complex network and diverse datasets across widespread data sources. The traditional cybersecurity solutions becoming ineffective and inadequate to resolve unforeseen challenges paused by widespread threat vectors discussed in above sections.

This study utilising state-of-the-art reference model and solution- it can enable cyber-secure internet and digital technologies usage along with underlying data network and information systems in the multi-organisational environment. In this paper, we are proposing a robust optimisation approach that seeks a solution to detect and protect against advanced cybersecurity challenges by leveraging the benefits of big data security intelligence with fast data technologies. The novel approach helps to leverage the benefits of distributed data storage, supporting diverse datasets including unstructured and steaming data and fast data processing. The paper is presenting a technology-independent reference model utilising said cutting-edge sciences for the cybersecurity analytic systems.

The research studies and outcomes consolidated with 'proof of concept' within critical information infrastructure (CII) and communication, the data analysis and results will be published in the future long paper. The research work is adding values in our previous rigorous research work of the last eight years within the fields. Although this robust cybersecurity solution implied and deployed in one field, the application in other field requires careful inspection. There is also a potential to consolidate our proposed solutions with an addition of social sciences, human behaviour and response. In the future, these outcomes can be explored and closely observe in other fields; this will further evolve, strengthen and consolidate the cybersecurity for safer and secure societies and businesses.

Acknowledgment

The reported research work is part of research, innovation and working-life projects including RIESCA, SATERISK, MOBI, MACICO, ABC4EU, European Common Information Sharing Environment (CISE) including FinCISE and EUCISE2020, Cybersecurity Economics and Analysis (CEA), and development work. The project and research work been facilitated by Laurea University of Applied Sciences and the University of Jyväskylä, Finland. These projects and relevant development work been carried with more than 50 governmental, industrial, academic and research organisations. For the financial and process support for research studies and relevant work, we would like to thank the Finnish Funding Agency for Technology and Innovation (Tekes), European Innovation Funding schemes including FP7 & H2020, Finnish Emergency Services and Police Authority, European Cybersecurity Organisation, Laurea University of Applied Sciences and University of Jyväskylä. This work been partly supported by one or more entities mentioned above. The research work becoming useful and positive endouvers with the support of our colleagues and research team worked with. We thank you all.

References

Alaba, F.A., Othman, M., Hashem, I.A.T. and Alotaibi, F. (2017) Internet of Things security: A survey. Journal of Network and Computer Applications, 88, pp.10-28.

Ani, U.P.D., He, H. and Tiwari, A. (2017) Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective. Journal of Cyber Security Technology, 1(1), pp.32-74.

Babiceanu, R.F. and Seker, R. (2016) Big Data and virtualization for manufacturing cyber-physical systems: A survey of the current status and future outlook. Computers in Industry, 81, pp.128-137.

Bachmann, F., Bass, L., Klein, M. and Shelton, C. (2005) Designing software architectures to achieve quality attribute requirements. IEE Proceedings-Software, 152(4), pp.153-165.

Bendovschi, A. (2015) Cyber-attacks–trends, patterns and security countermeasures. Procedia Economics and Finance, 28, pp.24-31.

Bengtsson, L., Borg, S. and Rhinard, M. (2018) European security and early warning systems: from risks to threats in the European Union's health security sector. European Security, 27(1), pp.20-40.

Brookson, C., Cadzow, S., Eckmaier, R., Eschweiler, J., Gerber, B., Guarino, A. and Rannenberg, K. (2015) Definition of Cybersecurity-Gaps and overlaps in standardisation. ENISA.

Bazarkina, D. (2019) February. Advanced Technologies Combating Terrorism in the EU: The Psychological Warfare Aspect. In ICCWS 2019 14th International Conference on Cyber Warfare and Security: ICCWS 2019 (p. 23). Academic Conferences and publishing limited.

Camhi, J. (2015) BI Intelligence projects 34 billion devices will be connected by 2020. Business Insider, 6.

Carcary, M., Doherty, E. and Conway, G. (2019) A Framework for Managing Cybersecurity Effectiveness in the Digital Context. In European Conference on Cyber Warfare and Security (pp. 78-XIII). Academic Conferences International Limited.

Carroll, J. (2019) July. Leveraging the OODA Loop with Digital Analytics to Counter Disinformation. In European Conference on Cyber Warfare and Security (pp. 106-XII). Academic Conferences International Limited.

Chen, H.M., Kazman, R., Monarch, I. and Wang, P. (2017) Can Cybersecurity Be Proactive? A Big Data Approach and Challenges. In Proceedings of the 50th Hawaii International Conference on System Sciences.

Du, P.Y., Zhang, N., Ebrahimi, M., Samtani, S., Lazarine, B., Arnold, N., Dunn, R., Suntwal, S., Angeles, G., Schweitzer, R. and Chen, H. (2018) November. Identifying, Collecting, and Presenting Hacker Community Data: Forums, IRC, Carding Shops, and DNMs. In 2018 IEEE International Conference on Intelligence and Security Informatics (ISI) (pp. 70-75). IEEE.

Eling, M. and Wirfs, J. (2019) What are the actual costs of cyber risk events?. European Journal of Operational Research, 272(3), pp.1109-1119.

Evans, M.R., Oliver, D., Yang, K., Zhou, X., Ali, R.Y. and Shekhar, S. (2019) Enabling spatial big data via CyberGIS: Challenges and opportunities. In CyberGIS for geospatial discovery and innovation (pp. 143-170). Springer, Dordrecht.

Finnerty, K., Motha, H., Shah, J., White, Y., Button, M. and Wang, V. (2018) Cyber Security Breaches Survey 2018: Statistical Release.

Hafsa, M. and Jemili, F. (2019) Comparative Study between Big Data Analysis Techniques in Intrusion Detection. Big Data and Cognitive Computing, 3(1), p.1.

Haldorai, A. and Ramu, A. (2018) The impact of big data analytics and challenges to cyber security. In Handbook of Research on Network Forensics and Analysis Techniques (pp. 300-314). IGI Global.

Huskaj, G. (2019) The Current State of Research in Offensive Cyberspace Operations. In 18th European Conference on Cyber Warfare and Security (ECCWS 2019), 4-5 July 2019, Coimbra, Portugal (pp. 660-667). Academic Conferences and Publishing International Limited.

Ishikiriyama, C.S. and Gomes, C.F.S. (2019) Big Data: A Global Overview. In Big Data for the Greater Good (pp. 35-50). Springer, Cham.

Kabir, M.F. and Hartmann, S. (2018) May. Cyber security challenges: An efficient intrusion detection system design. In 2018 International Young Engineers Forum (YEF-ECE) (pp. 19-24). IEEE.

Karchefsky, S. and Rao, H.R. (2017) Toward a safer tomorrow: Cybersecurity and critical infrastructure. In The Palgrave Handbook of Managing Continuous Business Transformation (pp. 335-352). Palgrave Macmillan, London.

Katal, A., Wazid, M. and Goudar, R.H. (2013) August. Big data: issues, challenges, tools and good practices. In 2013 Sixth international conference on contemporary computing (IC3) (pp. 404-409). IEEE.

Madan, B.B., Gogeva-Popstojanova, K., Vaidyanathan, K. and Trivedi, K.S. (2002) June. Modeling and quantification of security attributes of software systems. In Proceedings International Conference on Dependable Systems and Networks (pp. 505-514). IEEE.

McAbee, S.T., Landis, R.S. and Burke, M.I. (2017) Inductive reasoning: The promise of big data. Human Resource Management Review, 27(2), pp.277-290.

Mtsweni, J. and Mutemwa, M. (2019) July. Technical Guidelines for Evaluating and Selecting Data Sources for Cybersecurity Threat Intelligence. In European Conference on Cyber Warfare and Security (pp. 305-XVI). Academic Conferences International Limited.

Rajamäki, J., Rathod, P. and Holmström, J. (2013) August. Decentralized fully redundant cyber secure governmental communications concept. In 2013 European Intelligence and Security Informatics Conference (pp. 176-181). IEEE.

Rajamäki, J. and Simola, J. (2019) How to Apply Privacy by Design in OSINT and big Data Analytics?. In European Conference on Cyber Warfare and Security (pp. 364-XVIII). Academic Conferences International Limited.

Ren, S., Zhang, Y., Liu, Y., Sakao, T., Huisingh, D. and Almeida, C.M. (2019) A comprehensive review of big data analytics throughout product lifecycle to support sustainable smart manufacturing: A framework, challenges and future research directions. Journal of cleaner production, 210, pp.1343-1365.

Thomas, J.J. (2005) Illuminating the path:[the research and development agenda for visual analytics]. IEEE Computer Society.

Ullah, F. and Babar, M.A. (2019) Architectural Tactics for Big Data Cybersecurity Analytics Systems: A Review. Journal of Systems and Software, 151, pp.81-118.

Velásquez, W., Munoz-Arcentales, A. and Salvachúa, J. (2018) January. Fast-data architecture proposal to alert people in an emergency. In 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 165-168). IEEE.

Wampler, D. (2018). Fast Data Architectures for Streaming Applications. O'Reilly Media, Incorporated.

Professor Paul W. Poteete teaches information systems and cybersecurity programs at Geneva College. Previously, Professor Poteete worked in New Zealand, the United Arab Emirates, Hawaii, and California in executive leadership roles in industry and faculty roles at several schools. He graduated from the United States Naval Postgraduate School while providing research and joint operations support.

Dr. Dorothy Potter has over 20 years of experience as a Federal Financial Manager. As a Professor of Practice, she currently teaches for the National Defense University College of Information and Cyberspace and is Lead Faculty for the Risk Management, Internal Controls, and Auditing for Leaders graduate course, and provides teaching support to other faculty.

Dr. Paresh Rathod has worked more than 18 years in the fields of ICT and international businesses. Currently, Dr. Rathod is working as a senior lecturer at Laurea UAS, Finland. He is also serving as a Chairman of European Cybersecurity Organisation (ECSO), Brussels. He is actively working in the European and International Research, Development & Innovation (RDI) and business projects.

Dr. Aunshul Rege is an Associate Professor with the Department of Criminal Justice at Temple University. Her cybercrime/security research on adversarial decision-making and adaptation, organizational and operational dynamics, and proactive cybersecurity is funded by several National Science Foundation grants.

David M. Rohret is the lead Research and Development scientist for GDIT's full spectrum cyber red team. He received his Master's in Computer Science from LaSalle University in 1994. He has presented and published in over 25 technical conferences and journals. His current areas of research are autonomous offensive AI systems and alternate coupling effects.

Dr. Joseph H. Schafer is Professor and Chair of Leadership and Strategy, College of Information and Cyberspace, NDU, USA. Joseph has BS in EE & CS from West Point, MS and PhD in CS from GWU, MA in Strategy from Naval War College, and MBA from UVA Darden. His current research focuses on the security implications of influence and strategically disruptive emerging technologies.

Dr. D. Cragin Shelton, CISSP, has experience in supply chain risk management, electronic health system security, insider threat monitoring, identity management, PKI, and network boundary protection. His degrees are in cybersecurity, information systems management, and chemistry. He is a Senior Member of IEEE and ISSA, and a member the Computer Society, (ISC)2, and INCOSE.

Jantje Silomon is a researcher at the Institute for Peace Research and Security Policy in Hamburg (IFSH), having joined as part of the Arms Control and Emerging Technologies Research Project in 2019. Previously, she conducted her doctoral research on the topic of software as a weapon at the University of Oxford.

Jussi Simola works as a DSS specialist in Laurea University of Applied Sciences and he is a PhD student of cyber security in University of Jyväskylä. His area of expertise includes decision support technologies, SA systems, information security and continuity management. His current research is focused on effects of cyber domain as part of Hybrid Emergency Response Model.

Risto Vaarandi received his PhD degree from Tallinn University of Technology (Estonia) in 2005. In 1998-2018, he was affiliated with SEB Estonia and NATO CCDCOE, and since 2015, he is working as a senior researcher in Tallinn University of Technology. His research interests include event correlation, event log mining and analysis, and security monitoring technologies.

Petri Vähäkainu is a project researcher (MSc., BSc.) in Faculty of Information Technology at the University of Jyväskylä in Finland. He has been researching utilization of Artificial Intelligence in Cyber Security, health care and Structural Health Monitoring.

Dr. Cihan Varol is an Associate Professor of Computer Science at Sam Houston State University. He received his Ph.D. in Applied Computing from University of Arkansas at Little Rock in 2009. His research interests are in the general area of information (data) quality and its applications on Digital Forensics and Information Security areas.