International Journal of Economics, Commerce and Management
United Kingdom ISSN 2348 0386 Vol. VII, Issue 4, April 2019

http://ijecm.co.uk/

SMART CITIES REAL-TIME CYBERSECURITY COHESION USING JULIA LANG

Antonio CLIM
Faculty of Cybernetics, Statistics and Economic Informatics, Department of Economic Informatics and Cybernetics, The Bucharest University of Economic Studies, Romania
antonio.clim@csie.ase.ro

Abstract

The threat of cyber-attacks is imminent given the sophisticated technology especially that is used by the cybercriminals. It is therefore incumbent on governments and municipalities to ensure that even as they implement the smart cities using the associated technologies, they guarantee real-time cybersecurity. A real-time cybersecurity using Julia's version 1.1 has the potential to improve, monitor smart cities, and sensor environments. As the language that is designed for Data Science and machine learning, Julia has made in-depth research while at the same time guaranteeing performance. Further, Julia is the language that is designed for the users to ship the fancy algorithms in data science without necessarily having to rewrite these data on another word. Monitoring of smart cities using appropriate technologies will potentially help solve various challenges that are exposed to the progression of smart cities. With the use of Julia as a language for programming, it will be possible to detect some of the cyber threats that are exposed to the systems that are interconnecting smart cities. A qualitative research analogy was used in the methodology with the research adopting a secondary approach where a close analysis and reference was made on previous studies that have been conducted in the past.

Keywords: Julia Lang 1.1, Real-time Cybersecurity, Smart Cities, Hadoop, Big Data analytics, Public administration

INTRODUCTION

Julia Lang is the new language that aims to enhance the performance of C and the simplicity of Python. With the ability to conduct data analysis effectively with less trouble, Julia ensures that the shipping of the code has a competitive performance. Julia is additionally expected to be a significant tool in FinTech businesses (Buyya & Dastjerdi, 2016). A real-time cybersecurity using Julia's version 1.1 has the potential to improve, monitor smart cities, and sensor environments. As the language that is designed for Data Science and machine learning, Julia has made in-depth research while at the same time guaranteeing performance. Further, Julia is the language that is designed for the users to ship the fancy algorithms in data science without necessarily having to rewrite these data on another word (Bunz & Meikle, 2018). The research is concerned with real-time cybersecurity using Julia Lang version 1.1 just as any other programming language ensures that there is an incorporation of database systems in managing the applications in smart cities. An explosion in the number of smart, connected and the inherently insecure devices has shifted the security paradigm (Weber & Weber, 2010). Even though the Internet of Things is likely to ensure a technological shift, some alternative approaches should be developed in the process (Dameri, 2017). In as much as smart cities continue to sprout, security and privacy have been cited for impeding the progress of technological advancements.

Privacy and security of the real-time data as shared by various interconnected systems and communication devices in the afore mentioned smart cities need to be guaranteed. It will ensure non-interference of communication in those urban places (Martin, 2014). Cybercriminals are likely to hack into the lively city systems and cause confusion within the traffic system or even cause havoc by stealing crucial information from the internet. Similarly, the Internet of Things estimates that by 2020, nearly 50billion devices will be connected and they shall exchange and collect personal data regarding the users their tastes and preferences (Kott, Wang, & Erbacher, 2014). Government organisations are more vulnerable to cyber-attacks especially when they are connected to the Internet of Things. It calls for cyber protection on a real-time basis so that sophisticated cyber-attacks could be detected as early as possible.

SIGNIFICANCE OF RESEARCH

The research on real-time cybersecurity using Julia for smart cities is significant as it will help solve security and privacy issues. Such entails the collaboration of data and information collectively shared with the Internet of Things (IoT). With the analysis of various capabilities and the conceptualisation of the smart cities concept, solving security and privacy problems that could potentially affect the operation of smart cities.

The security cases, for instance, a targeted distributed denial of service (DDoS) attacks on the power grids and the industrial control systems are on the rise. Real-time cybersecurity by Julia Lang will help in detection of the vulnerabilities that are exposed to the smart city systems (Gupta, Agrawal, Yamaguchi, & IGI Global., 2016).

Cybercriminals are using big data in mining big data from corporations for their illicit gains. They are additionally utilising this tool in monitoring their various interrelated processes while at the same time improving their efficiency (Buyya & Dastjerdi, 2016). They will apply the use of big data in gaining information on databases that have been breached, the compromised information systems as well as machines that are infected with viruses.

STATE OF THE ART

Over the past two decades, the concept of Smart City has wholly transformed the urban life, which involves the sectors for instance transport, energy, health as well as education. Various governments have embraced the concept of smart cities as a strategy to improve the citizen's living standards and the application of big data. The applications for the lively city have the potential of transforming each sector of the economy (Heard, Adams, Rubin-Delanchy, & Turcotte, 2019). Real-time monitoring and surveillance in towns and major urban roads could potentially track traffic and other crimes on a real-time basis. Additionally, monitoring significant areas in the city could detect suspicious activities for the critical infrastructures, which will provide for capabilities to quickly respond to emergencies (Gupta, Agrawal, Yamaguchi, & IGI Global., 2016). These transformations enable municipalities and cities to adopt various learning principles as well as the prerequisites for the necessary applications in smart cities.

A smart environment plays a significant role in smart cities. An epitome of an intelligent climate contains the resilience, governance, improved quality of life as well as collaboration with the authorities (Bibri, 2018). Brilliant managing of the existing natural resources and the city facilities. It will require efficient management of the information at the disposal of the authorities that are mandated to monitor the related systems in these smart cities (Urquhart & McAuley, 2018). Maintenance of a bright environment will be substantial, as it will help protect the critical infrastructure that is used in the facilitation of monitoring and surveillance systems in smart cities(Rodríguez, 2015). Such cannot be done in a vacuum thus the need for the use of the internet in the real-time management of smart cities. Some vulnerabilities are associated with the use of the internet, which involves cybersecurity and related threats.

Technology has led to a fundamental shift in the way people go about their businesses including governments. While it offers various opportunities for innovation and productivity, the cyber era comes with risks and challenges (Gupta, Agrawal, Yamaguchi, & IGI Global., 2016)).

From businesses to their employees and customers, citizens and governments, each is exposed to cyber risks. With the interconnection of systems in smart cities and the need for collaboration with all the stakeholders, the magnitude of a threat or a risk could affect significant players when it is experienced (Bibri, 2018). The cyber supply chain has eliminated the first traditional security perimeter, for instance, the enterprise adopt cloud, social as well as mobile technologies and an investment in the third-party business relationships (Bibri, 2018). As guaranteeing perfect security could be quite a challenge, an agile and a pragmatic approach is necessary for the growth as well as innovation to progress in the present modern world (Bibri, 2018).

The cyber ecosystem is complex and is regarded as growing on a fast trajectory. In as much as it is necessary to invest in security, incidents may or may not occur. However, rapid response is critical for minimising financial loss and damage of brands (Gilchrist, 2017). Julia Lang version 1.1 is among the cyber intelligence systems that will ensure that there are real-time surveillance and protection of the critical methods for enabling the functioning of smart cities (Bibri, 2018).

Development of smart city projects requires different citizens, physical infrastructure, economic activities, stakeholders, housing services, utilities as well as technologies that are working together. Kumar et al. (2018) have provided a Smart City Transformation Framework (SCTF) in presenting how the critical services for the smart cities could be integrated as well as the technological solutions that can help in enabling such transformation(Mohanty, Jagadeesh, & Srivasta, 2013). The findings of this study confirm that the integration of the infrastructure can help improve service delivery as well as efficiency. Application of software integration techniques helps in improvement of network capabilities and at the same time ensuring the security of critical systems that are used in the integration of smart city systems (Andreev, Balandin, & Koucheryavy, 2012).

Cisco Systems are amongst the largest manufacturers and developers of telecommunication systems and network hardware equipment. Cisco Systems tailors the machine learning algorithms for computer security by network data, steganalysis and steganography in the detection of the computers that are affected.

Construction of smart cities is likely to bring about the higher quality of life to a majority of people through the digital interconnectivity, which leads to increased efficiency as well as accessibility in these cities. Smart cities need to ensure that there is individual privacy as well as security to facilitate participation by the citizens (Gilchrist, 2017). Some of the challenges to smart cities participation include the preservation of privacy with the high dimension data, securing of networks that has a large surface for attack, establishment of data sharing

capabilities and practices, proper use of artificial intelligence as well as mitigating failures that are cascaded through the smart networks (Gupta, Agrawal, Yamaguchi, & IGI Global., 2016). In the construction of intelligent cities, these are all systems that need to be observedto guarantee reliability and security of personal data(Sohal, Sandhu, Sood, & Chang, 2018). Real-time monitoring of cybersecurity is thus necessary so that the data that is shared across these networks can be secure and free from any attack by hackers and other malicious users.

METHODOLOGY

A qualitative methodology was used in the real-time cybersecurity using Julia language. The research analysed past studies that have been done on this element of big data applications in cybersecurity and at the same time conceptualising various factors in Julia and its usefulness in the smart cities (Heard, Adams, Rubin-Delanchy, & Turcotte, 2019). The analysis and conceptualisation of Julia as a programming technique is critical as it helped in the understanding of the research and a review of the underlying technologies that are required for the smart cities. Data used in this study were the data that are analysed from the secondary research sources and analysis drawn therein (Andreev, Balandin, & Koucheryavy, 2012)

Design science is the methodology that was used in studying real-time cybersecurity using Julia for smart cities. In modelling the entire Internet or a portion of it, there is a need for the implementation of a learnable message-passing algorithm for the graph with Flux.jl. Julia is scalable as it ensures that there is real-time cybersecurity in smart cities. In the design and implementation of smart cities, a lot of information will be needed by the stakeholders that are involved (Gilchrist, 2017). It is therefore critical to ensure that a framework is developed for protecting the security of the information held in the database of these smart cities. It is by real-time protection of data that cybersecurity and protection of the critical infrastructure of smart cities will be guaranteed(Kott, Wang, & Erbacher, 2014). Julia Lang helps in writing efficient code in a single language thus no need for combinations for instance Python + TensorFlow + C. Julia Lang is the dynamic programming language that has been designed to address high performance needs as well as numerical analysis and computational science. The language provides for the sophisticated compiler, numerical analysis, distributive parallel execution as well as an extensive mathematical function.

Real-time Cybersecurity using Julia for Big Data

The scientific computing has required high performance, but the domain experts have resorted to slower dynamic languages to enhance their daily work. However, researchers believe that there are more good reasons for preference on dynamic languages for the applications, thus,

not expecting the use to diminish (Gupta, Agrawal, Yamaguchi, & IGI Global., 2016). The modern language, as well as the, fortunately, y makes it possible to do away with the performance trade-off thus providing for an environment that is productive enough to prototype and deploy applications that are performance-intensive (Salceanu, 2018). It is for this reason that the use of Julia Lang in smart cities in controlling traffic and managing other functions, which are performance intensive, is vitally thus critical.

Julia is designed to enable future capabilities and uses just as MATLAB was designed to handle complex matrix calculations (Andreev, Balandin, & Koucheryavy, 2012). Programmers always use tools, which translates slower languages, for instance, Ruby and Python into faster language like C or Java. However, the quicker code needs to be explained as well or compiled in the programmer lingo, which is the code that could be better understood by the machine(Mainka, 2018). Julia is unique and different from the other programs in that it does not require an intermediary step. Using LLVM, which is a compiler that was developed by the University of Illinois, a language is built that compiles the data straight into machine code even as it is on the run (Andreev, Balandin, & Koucheryavy, 2012)

Julia programming language is the dynamic language that is appropriate for the scientific as well as numerical computing with its performance being comparable to the traditional languages, which were statistically, typed (Dameri, 2017). By a sophisticated compiler, a distributed parallel execution, numerical accuracy and the extensive mathematical function, Julia is in a position of providing real-time cybersecurity. This is enabled by providing analysis into the activities of smart cities and the related system.

Additionally, Julia analyses the activities of the related system to devise a better strategy for addressing pitfalls in privacy and security whenever they are experienced (SmartCom & Qui, 2017). With the extensive mathematical library function, Julia potentially analyses an action and gives real-time feedback on how the action could be mitigated. One might find the performance of Julia as being unintuitive at first because of the fact that its compiler is entirely different from those of Python and R. Writing a code especially for smart cities using Julia is easy as data that is needed are collected from the devices that are located at specific points in these cities under analysis (Hostettler, Najih, & Bolay, 2018). Julia is multi-paradigm while at the same time, it combines the features of imperative, functional as well as programming that is object-oriented and data-centered (Andreev, Balandin, & Koucheryavy, 2012). This language not only provides the ease and expressiveness for the high-level numerical computing but also it supports the general programming just as is done by Python, Java and R. In achieving this, Julia Lang build up on the lineage of the languages used in mathematical programming and at the same time borrows heavily from a set of dynamic languages such as Lisp, Lua and Ruby.

Julia programming is aimed at the creation of the unprecedented combination of the easy-to-use, powerful and efficient systems in a single language (Nicopolitidis, 2016). Some of the advantages of using Julia include:

i. It is a free and an open source
ii. It has powerful shell-like capabilities that help to manage an array of processes.
iii. It is designed for parallelism and distributive computing
iv. It is efficient and supports Unicode which includes but not limited to the UTF-8(Hasib, 2014).

Through inserting sensors across critical infrastructure in cities as well as the creation of new data sources, which is inclusive of citizens and their mobile devices, the smart city managers, will apply Big Data analysis in monitoring and anticipation of the urban phenomena.

Allowed Variable Names in Julia

Variable names in Julia must begin with letters (A-Z or a-z), an underscore or a given set of Unicode points that is greater than 00A0, and in particular Lu/LI/Lt/Lm/Lo/NI. Sc/So and a few other characters that are letter-like for instance Sm which is a subset of a math symbol are allowed in the Julia programming (Hasib, 2014)). Subsequent characters in Julia could also include '!'as well as digits'(0-9') and other Unicode code points, diacritics and other modifying marks are also used in the Julia programming. Operators, which includes + are also valid identifiers but are usually parsed. In some instances, operators are most likely to be variables for instance (+) refer to an addition function, but (+) = £ will help in reassigning the function. These are all operators that are critical to the development of a Unicode code and helps in developing the Julia code (Maglaras, Janicke, & Jones, 2017). With the real-time data processing capabilities of smart cities, it will be essential to define the scope of Julia code and its basic applications to the security and privacy of the database of smart cities.

The Cybersecurity Threat Concept

Cybersecurity threats arise because of the development of more sophisticated advancement in technology. Exemplary attempts have been made over the past to try to analyse the entire issue of cybersecurity from a more enhanced perspective with the aim to attempting to achieve maximum protection for systems in organisations and especially the smart cities (Bunz & Meikle, 2018). This research is aimed at suggesting some of the practical measures that when put in place could help in solving some of the cybersecurity challenges that smart cities have been facing over the past in a bid to ensure that they guard their systems from external attacks by malicious attackers (Dameri, 2017). Information sharing is additionally seen to be a very

crucial aspect in cybersecurity as the various stakeholders need to share relevant information promptly which helps in ensuring that various models in a business can be applied to help salvage a situation.

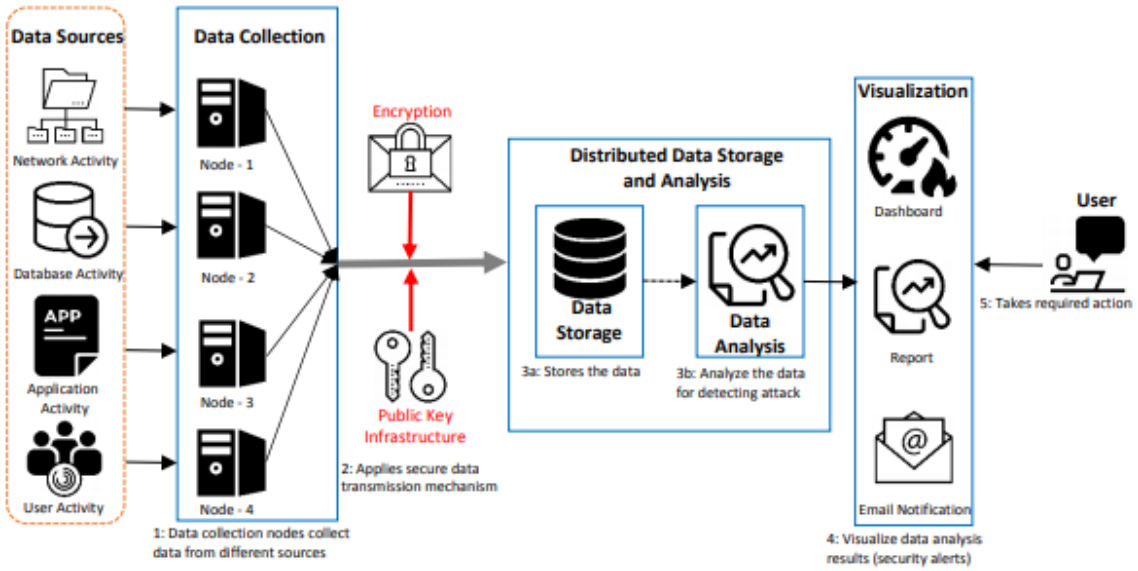
Big Data Analytics in Cybersecurity

According to Fischer (2016), there are several Big Data projects, which are developed to deal with the threat of cyber, which is a threat that nearly all organisations face. Platfora is the big data analytics platform that has been built on the Apache Hadoop. Platfora helps in providing for a platform in which various security events, as well as pattern processing, will be enabled to help in the identification of malicious activities (Fischer, 2016). Companies, for instance, Niara are presently in the process of developing various cybersecurity tools using Hadoop Cluster. Big data is one of the aspects that are seen to be a double-edgedd sword to cybersecurity. With the increase in the cyber threats, big data will help prevent adversaries from taking advantage of the massive amount of information, trade secrets or even the personal and the financial data that is available (Fischer, 2016). Big data is an emerging security measure aimed at ensuring that the cyber threats that an organisation faces have been eliminated significantly (Ullah & Babar, P., 2018). There is a consistent encouraging of organisations to transition from traditional security systems to the intelligence-driven security, which provides a broader view of the vulnerabilities and the risks that an organisation faces (Kott, Wang, & Erbacher, 2014). It will require an analysis of the external threat intelligence feeds, the calendars that are cloud-based and the logs within the social network activity (Akhgar, 2015). An advantage with big data is that it can to do an analysis of massive security events and establish a connection with the aim of prioritising the threats (Andreev, Balandin, & Koucheryavy, 2012). In the smart cities, prioritising the threats is critical as this helps in providing a real-time solution to the cybersecurity challenges that are predisposed to the efficiency of smart cities. A collaborative information systems approach ensures that enough data has been analysed with the aim of improving the smart city system.

With the use of big data, the disparate pieces of data are likely to connect and provide the cybersecurity professionals with a clear picture of a security situation (Singh & Kumar, 2016)). The research established that this very same idea of Big Data in providing solutions to the cybersecurity challenges could be applied in smart cities in ensuring that there is a set-up of a strong and a resilient framework for these cities (Kott, Wang, & Erbacher, 2014). When establishing a city, it is evident that there is a need for guaranteeing of various security measures in a bid to improve as well as enhance the interconnected systems and process and at the same time ensure that the security of these cities has been significantly considered (Siegel, 2012). Therefore, in future, there will be a need for the building an urban framework that

incorporates the critical security issues through design by the use of big data architecture (Fischer, 2016). From an observation point of view, it was possible to evaluate some of the factors that lead to cyber threats in organizations, however, the researcher established that most of the security threats are caused by the employees themselves as some always tend to bypass the security measures and protocols that have been established in organizations (Singh & Kumar, 2016). The Hadoop framework will provide ease of collection as well as the storage of massive data amounts through which various analytic techniques could be used in the identification of malware (Fischer, 2016). It will help in addressing the issue of breach in data as the Hadoop framework will collect, sort and store large amounts of data after an analysis has been done to ensure that no malware exists in the data, which could potentially affect smart cities (Savas & Deng, 2017).

Figure 1: Cybersecurity schemas for a Smart City(Nicopolitidis, 2016)



Big data analytics is regarded as a must-have component for the effective real-time cybersecurity solution because of the need to process the high velocity and high volume of data that comes from various sources discover anomalies as fast as possible and limit the vulnerability of the system(Bunz & Meikle, 2018). Such will help increase the resilience of the system and deter any possible threats that are exposed to the smart city systems.

IMPLICATIONS FOR PRACTICE

Information technology (IT) plays a critical role in the smart cities through making the data collected through the information technology components available for use by the various

stakeholders. This technology is what is referred to as the Internet of Things (IoT), and it works through communicating with the connected devices while at the same time exchanging data which requires the use of the internet, wireless technologies as well as other mediums of communication (Ustundag & Cevikcan, 2018). Using Julia Lang in smart cities implies that cybersecurity concept is likely to be enhanced with the government and authorities being in a position to potentially control some of the functions that are related with smart cities (Akhgar, 2015). Better-coordinated traffic and surveillance of crimes is an example of some of the capabilities that are associated with smart cities (Weber & Weber, 2010). Smart cities often make use of the sophisticated IoT devices in fetching data as well as effectively processing this data for the implementation in a given particular region (Ustundag & Cevikcan, 2018).The smart city sensors, as well as the connected devices, collect data from the different smart city gateways that are installed in the city and analyse this information to make better decisions as a result.

The development of smart cities goes beyond the standard practices of phasing out conventional technology. Instead, the development of smart cities aims at adding sensors, remote supervision and controlling some of the crucial components in the city (Haidine, El Hassani, Abdelhak, & El Hannani, 2016). Julia Lang technology provides the necessary solution as it considers real-time information to rein control.

Additionally, the language brings in the concept of having a sustainable environment. Technology applied at smart cities should be parallel to the needs of the occupants. Energy consumption is one of the crucial components of urban spaces (Przeybilovicz, Cunha, Macaya, & De Albuquerque, 2018). Therefore, smart cities should be in a position to create sustainable cities and optimise energy uses.

IoT has become an integral infrastructure since the conceptualisation of smart cities. Most of the focus of smart cities has been shifted to the collection of data to determine the needs of the environs (Hasbini, Eldabi, & Aldallal, 2018). IoT is concerned with the collection of information from various electronic, storing it and augmenting it to useful information, even connecting m-Health data for medical emergencies situations, thus reducing public health costs through preventions plans (Tinică, Bostan, & Grosu, 2010). However, to achieve such efficiency, the ICT structure needs to relay information is an expedite manner (Park, del Pobil, & Kwon, 2018). Julia Lang language reduces the gap by providing an innovative solution for transmitting data in real time. The need for a sustainable environment in the cities leads to an urgent application of IoT. After developing the foundation for smart cities, it is essential to come up with services for data collection (Park, del Pobil, & Kwon, 2018). That is, IoT technologies related technologies allow for an effective manner of processing and using the data collected.

Smart cities consist of a complex chain of infrastructure conducting the flow of information. If the data is poorly handled, it could increase inconveniences in the town (Chamoso, González-Briones, Rodríguez, & Corchado, 2018). The technologies that are concerned with data transmission or integration create the core of urban engineering that is based on wireless sensors (Chichernea, 2015). The sensors allow for the combination of information from the social platforms and that of the physical aspect.

Additionally, the sensors create one of the essential components for analysing the different elements in an environment and creating important relations. The information from the sensors is collected due to the IoT devices that facilitate communication (Duda, Kunanets, Matsiuk, & Pasichnyk, 2018). For instance, smart noise controls are created with the function of detecting the levels of noise from different areas (Duda, Kunanets, Matsiuk, & Pasichnyk, 2018). As a result, the information is transferred to the main centre to determine if the sound is under the required threshold.

The sensors are integrated in such a manner that they each serve their intended purpose. Sensors utilising RFID are designed to identify the network objects while those with Wireless Sensor Networks (WSN) collect and sort the data generated in IoT structures (Lea, 2017). In essence, the entire process indicates that a communication platform is instrumental in the smart city environment. Therefore, while developing technology, it is essential to conceptualise a common language for the different sensors. For instance, the IPv6 protocol has an extended space that addresses the various IoT spaces (Duda, Kunanets, Matsiuk, & Pasichnyk, 2018). Consequently, the protocol probes the manageability and efficiency of using devices under limited resources. The Julia language aims at proving sustainable practices under minimalist perspectives.

Notably, the technologies created can generate different types of results depending on the institutional policies implemented. The technical solution provided cannot suffice alone without the local officials providing sustainable practices (Miklian & Hoelscher, 2017). Therefore, the use of ICT by the government can be instrumental in encouraging citizens to participate in innovative solutions. Furthermore, as the environs provide information, the state must be in a position to address the issue brought forward (Covell, 2016). In reality, smart cities are concerned with communication models. As they continue to develop, innovative practices will be required to create a cohesion of the existing entities.

FUTURE WORKS

The technology potentially provides capabilities to be explored in the future. For instance, the application of real-time cybersecurity with the use of Julia is in a position of enhancing smart

medical services in the future. The possibility of responding to emergencies in the future will be enhanced using smart medical services (Gilchrist, 2017). The research observes that it is the similar concept of smart cities that will be used in the designing of e-Ambulances in smart cities such that an emergency response is activated whenever there is a need(Ustundag & Cevikcan, 2018). With the real-time monitoring of the smart cities, emergency response will be initiated whenever the system detects and emergency which in effect will spur a response by the emergency medical services as well as the e-Ambulance systems(Lauwens, 2019). This requires the collaboration of all the stakeholders involved as the data that will be required in each instance will be crucial to the systematic development of smart medical services.

CONCLUSIONS

In short, Big Data analytics is among the measure that is used in ensuring that real-time cybersecurity using Julia as the programming language for smart cities sensor environments. Smart cities just as discussed in the research paper; rely on interconnectivity of dynamic information and the use of various robotic functions in enabling the functionality of the smart city systems. Smart cities are the future of cities. Therefore, the idea needs to be conceptualised with the framework for its implementation being developed as well. The threat of cyber-attacks needs to be eliminated to guarantee critical evaluation of data as well as other vital information areas in the organisation. Julia has capabilities that enable the development of effective smart city systems; however, with the integration of some crucial elements such as Big Data analytics in providing a real-time cybersecurity, it will be potentially possible to ensure that there is a protection as well as privacy and security being realized largely. The volume and magnitude of the information held by the smart cities systems are immense. In the event that a breach occurs, citizens who rely on such smart systems are likely to suffer with their data also being at risk. It is therefore incumbent upon governments to devise strategies and the efficient mechanisms for managing the integrity of the data while at the same time guaranteeing the usability of some critical infrastructure within the smart city systems.

REFERENCES

Akhgar, B. (2015). Application of Big Data for National Security. New York City.

Andreev, S., Balandin, S. I., & Koucheryavy, Y. (2012). Internet of Things, smart spaces, and next generation networking: 12th International Conference. Berlin: Springer.

Bibri, S. E. (2018). Smart sustainable cities of the future: The untapped potential of big data analytics and context-awarecomputing for advanced sustainability.

Bunz, M., & Meikle, G. (2018). The Internet of Things. New York City.

Buyya, R., & Dastjerdi, J. (2016). Internet of Things: Principles and Paradigms.

Chamoso, P., González-Briones, A., Rodríguez, S., & Corchado, J. M. (2018). Tendencies of Technologies and Platforms in Smart Cities: A State-of-the-Art Review. Wireless Communications and Mobile Computing, 49, 227–239. doi:https://doi.org/10.1155/2018/3086854

Chichernea, V. (2015). Smart cities communities and smart ICT platform. Journal of Information Systems & Operations Management, Volume 9 Issue 1.

Covell, C. (2016, December 29). A City Built on Information Technology and Wisdom: The Roles of the Government in the Establishment of the Smart Cities, Smart Communities. SSRN, 1-18. doi:http://dx.doi.org/10.2139/ssrn.2891184

Dameri, R. P. (2017). Smart city implementation: Creating economic and public value in innovative urban systems.

Duda, O., Kunanets, N., Matsiuk, O., & Pasichnyk, V. (2018). Information-Communication Technologies of IoT in the "Smart Cities" Projects. Proceedings of the 14th International Conference on ICT in Education, Research and Industrial Applications.2105, pp. 317-330. Kyiv, Ukraine: CEUR-WS.org. Retrieved from http://ceur-ws.org/Vol-2105/10000317.pdf

Fischer, E. A. (2016). Cybersecurity Issues and Challenges: In Brief. Congressional Research Services.

Gilchrist, A. (2017). IoT Security Issues.

Gupta, B., Agrawal, D. P., Yamaguchi, S., & IGI Global. (2016). Handbook of Research on modern cryptographic solutions for computer and cyber security. Hershey: IGI Global/Information Science Reference.

Haidine, A., El Hassani, S., Abdelhak, A., & El Hannani, A. (2016). The Role of Communication Technologies in Building Future Smart Cities. In Smart Cities Technologies. IntechOpen. doi:10.5772/64732

Hasbini, M., Eldabi, T., & Aldallal, A. (2018). Investigating the information security management role in smart city organisations. World Journal of Entrepreneurship, Management and Sustainable Development, 14(1), 86-98. doi:https://doi.org/10.1108/WJEMSD-07-2017-0042

Hasib, M. (2014). Cybersecurity leadership: Powering the modern organization.

Heard, N., Adams, N., Rubin-Delanchy, P., & Turcotte, M. (2019). Data science for cyber security.

Hostettler, S., Najih, B. S., & Bolay, J.-C. (2018). Technologies for development: From innovation to social impact.

Kott, A., Wang, C., & Erbacher, R. F. (2014). Cyber defense and situational awareness.

Lauwens, B. E. (2019). THINK JULIA: How to think like a computer scientist. O'REILLY MEDIA .

Lea, R. (2017). Smart Cities: An Overview of the Technology Trends Driving Smart Cities. IEEE Advancing Technology for Humanity, 1-14. doi:10.13140/RG.2.2.15303.39840

Maglaras, L. A., Janicke, H., & Jones, K. (2017). Industrial Networks and Intelligent Systems: Second International Conference, INISCOM 2016, Leicester, UK, October 31? November 1, 2016, Proceedings.

Mainka, A. (2018). Smart world cities in the 21st century.

Martin, J. (2014). Information security analytics - finding security insights, patterns, and a.

Miklian, J., & Hoelscher, K. (2017). Smart Cities, Mobile Technologies and Social Cohesion in India. Indian Journal of Human Development, 11(1), 1-16. doi:10.1177/0973703017712871

Mohanty, S., Jagadeesh, M., & Srivasta, H. (2013). Big data imperatives: Enterprise big data warehouse, BI implementations and analytics. (Big data imperatives.). New York: Apress.

Nicopolitidis, M. O. (2016). Smart Cities and Homes .

Park, E., del Pobil, P. A., & Kwon, S. (2018). The Role of Internet of Things (IoT) in Smart Cities: Technology Roadmap-oriented Approaches. Sustainability, 10(5), 1-13. doi:10.3390/su10051388

Przeybilovicz, E., Cunha, M. A., Macaya, J., & De Albuquerque, J. (2018). A Tale of two "Smart Cities": Investigating the Echoes of New Public Management and Governance Discourses in Smart City Projects in Brazil. 51st Hawaii International Conference on System Sciences (pp. 2486-2495). Hawaii: HICSS. doi:10.24251/HICSS.2018.314

Rodríguez, B. M. (2015). Transforming city governments for successful smart cities .

Salceanu, A. (2018). Julia programming projects: Learn Julia 1.x by building apps for data analysis, visualization, machine learning, and the Web.

Savas, O., & Deng, J. (2017). Big data analytics in cybersecurity and IT management.

Siegel, J. E. (2012). Data proxies, the cognitive layer, and application locality: enablers of cloud-connected vehicles and next-generation internet of things.

Singh, M. K., & Kumar, G. D. (2016). Effective big data management and opportunities for implementation.

SmartCom, & Qui, M. (2017). Smart Computing and Communication. SmartCom 2017. Shenzhen , China.

Sohal, S. A., Sandhu, R., Sood, S. K., & Chang, V. (2018). A Cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments.

Tinică, G., Bostan, V., & Grosu, V. (2010). Correlations regarding the economic growth and the direct and indirect costs incurred by chronic diseases. Revista Romana de Bioetica (Romanian Journal of Bioethics), 8(3), 116-124.

Ullah, F., & Babar, P. (2018). Architectural Tactics for Big Data Cybersecurity Analytic Systems.

Urquhart, L., & McAuley, D. (2018). Avoiding the Internet of insecure industrial things.

Ustundag, A., & Cevikcan, E. (2018). Industry 4.0: Managing the digital transformation. Springer.

Weber, R. H., & Weber, R. (2010). Internet of things: Legal perspectives. Berlin: Springer.