JOURNAL OF CRITICAL REVIEWS

ISSN- 2394-5125 VOL 07, ISSUE 19, 2020

PARALLEL PROCESSING OF MULTIPLE LEVELS HETEROGENEOUS DATA FOR END-TO-END COLLECTION AND ANALYSIS WITH IOT SECURITY USING NOVEL ENCRYPTED CODE

Research Scholar - Bollepogu Venkateswarlu[1], Dr. Pramod Pandurang Jadhav[2]

Department of Computer Science & Engineering, Dr. A.P.J. Abdul Kalam University, Indore (M.P.) - 452010

ABSTRACT: Networks of the Internet of Things (IoT) nowadays find greater widespread in many domains. Particularities of creation of IoT make the problem of their security monitoring rather actual; it is caused by necessity of processing of big amounts of heterogeneous data in real time. The problem may be solved by means of implementation of the parallel system for security data processing within IoT on the fly basing on complex event processing (CEP) technology. A key prerequisite for enabling such approaches is the development of scalable infrastructures for collecting and processing security-related datasets from IoT systems and devices. This analysis introduces such a scalable and configurable data collection infrastructure for data-driven IoT security. It emphasizes the collection of (security) data from different elements of IoT systems, including individual devices and smart objects, edge nodes, IoT platforms, and entire clouds. The scalability of the introduced infrastructure stems from the integration of state of the art technologies for large scale data collection, streaming and storage, while its configurability relies on an extensible approach to modelling security data from a variety of IoT systems and devices. The approach enables the instantiation and deployment of security data collection systems over complex IoT deployments, which is a foundation for applying effective security analytics algorithms towards identifying threats, vulnerabilities and related attack patterns.

KEYWORDS: Data collection, Internet of Things, security monitoring

I. INTRODUCTION

In recent years we are witnessing a proliferation of Internet of Things (IoT) deployments, which are mainly driven by the rising number of internet connected devices that already amount to several billions [4]. This tendency is accompanied by an increase in the sophistication of IoT systems, due both to their increased scale and to the emergence of smart objects that exhibit semi-autonomous behavior, for instance, drones, robots and autonomous guided vehicles. In this landscape, IoT deployers are confronted with pressing security challenges, including more vulnerabilities and security attacks. The latter require new and more intelligent approaches to IoT security, notably approaches that are able to tackle complex, unpredictable and sometimes asymmetric attacks at scale [8].

In quest for novel approaches that can cope with this complexity, such approaches have been recently developed for specific types of IoT infrastructures such as Wireless Sensor Networks and smart grids and for specific types of attacks like malware detection and intrusion detection [1]. However, the current evolution of computation and storage technologies opens new horizons in the deployment and for IoT security.

The use of data mining techniques (such as machine learning) for security monitoring and analysis is perfectly aligned to mainstream IoT architectures, including relevant reference architecture models. For example, discusses the security perspectives of the Reference Architecture

Model for Industy4.0 (RAMI4.0) and concludes that cross cutting security monitoring and analytics functions should be deployed for all layers of RAMI4.0. Another example is the Industrial Internet Security Framework (IISF), which provides the security view of the reference architecture of the Industrial Internet Consortium (IIRA) [2] and specifies a "Security monitoring and analysis" building block. The latter captures data about the overall state of the IoT system including its endpoints and connectivity traffic, and, accordingly, analyses it to detect possible security violations or potential system threats. Similar data-driven monitoring and actuation functionalities are specified in the scope of the Reference Architecture (RA) of the OpenFog Consortium. This RA underlines also the importance of end-to-end security as an integral function of all different IoT scenarios and system elements, i.e., security support spanning from low layer silicon/fog devices to all upper software layers of the fog architecture. It follows that all of the above RAs specify the importance of data-driven security support that implements a "Monitor-Analyse-Act" cycle.

Key to successful implementations of such a "Monitor- Analyse-Act" cycle that is in-line with the aforementioned architectures is the specification of a scalable, configurable and responsive infrastructure for collecting and storing the security data to be analyzed. Due to the very large volume, variety and potentially high velocity of security data, such a data collection infrastructure should satisfy requirements similar to those expressed for BigData systems. In this paper we introduce a BigData oriented infrastructure for collecting, storing, managing and analyzing security data from IoT systems. The infrastructure addresses the scalability challenges outlined above, while being flexibly configurable in order to support security monitoring for different IoT systems. Furthermore, it incorporates intelligence and security contextual aspects. For example, the amount and rate of collected data may be dependent on certain security indicators.

The presented data collection infrastructure is part of a wider IoT security monitoring, analysis and actuating system, which is implemented in the scope of the Horizon 2020 Secure IoT project whose objective is to provide security services to target IoT systems that may be deployed across different platforms and administrative domains based on predictive analytics. Therefore, prior to presenting the detailed architecture of the data collection infrastructure, we put it in the wider context of the Secure IoT project. The overall Secure IoT platform provides the means for end-to-end security monitoring of an IoT system, including protection for all functional blocks and end points that it comprises. To this end, Secure IoT integrates advanced analytics that provide the means for identifying and anticipating attacks on internet-connected devices, including smart objects with dynamic behavior.

II. LITERATURE SURVEY

M.-J. Kim and Y.-S. Yu et.al [5] explained the choice of Hadoop by the fact that this tool is currently pro most favorable for Big Data processing. It is Java-based framework with the Apache open source process, and it uses a relatively simple program model. The architecture of the wh proposed system includes Event Adaptor, CEP Analysis Engine, and Report & Event Generator. The system is aimed eng at sharing with the medical institution ERP systems. The CE Analysis Engine contains Event Collector, Data Analyzer, and Storage Server.

N. Zygouras, N. Zacheilas, V. Kalogeraki, D. Kinane, and D. Gunopulos et.al [6]

presents an CEP system designed for big data processing for traffic management. The proposed system combines two approaches: CEP and Distributed Stream Processing Systems (DSPS). CEP is supported by Esper system. DSPS approach is supported by Storm system. Hadoop plays a role of integrator, combining these two approaches. In addition. Hadoop provides historical data analysis. Experimental evaluation demonstrated high scalability of the system. However, in our opinion, its use to monitor loT is hindered by high computational requirements. At the same time, the achieved performance values of the system will guide our work.

N.P. Schultz-Meller, M. Migliavacca, and P. Pictzuch et.al [7] presents a CEP system in which High-Level Event Query Language is implemented which is close to SQL. For this language the authors developed algorithms for query optimization. The optimization criterion is the minimum time of the processor load.

H. Zhang, Y. Diao, N. Immerman et.al [9] presents a core language for pattern queries in CEP, which allows to process complex queries more quickly. However, the wide use of these systems for monitoring of IoT networks is difficult as it requires additional software tools that support these query languages.

A. Moraru and D. Mladenić et.al [12] explained framework for integrating CEP and data pe mining methods is discussed. As a use case the authors consider the smart cities scenario. For this reason, this work is of interest as an example of the application of CEP in IoT dat networks. The scenario contains a module of data integration and preprocessing, which performs data mining. However, in our opinion, the suggested approach requires significant computational costs. Therefore, these results are of limited use.

D. Gyllstrom, E. Wu, H.-J. Chae, Y. Diao, P. Stahlberg, and G. Anderson et.al [10] considers the CEP system designed for collection, cleaning, and processing of RFID data. The results of the processing of event streams in this system are stored in MySQL database. Despite the fact that this work is a good example of the successful implementation of CEP technology in IoT networks, it cannot be used for IoT security monitoring as the issues of parallel processing of big data were not considered.

D. Anicic, S. Rudolph, P. Fodor, and N. Stojanovic et.al [13] describes a system which enables specification and monitoring of complex event patterns in near real time and performs reasoning over streaming events. However, despite the fact that both proposed framework are feasible, the issues of preliminary event processing based on parallel computing in these papers were not considered.

D. Wang, E.A. Rundensteiner, and R.T. Ellison et.al [14] suggests a framework called Active CEP, which realizes the correctness of concurrent stream execution by embedding active rule support within the CEP engine. Active rules help to maintain the integrity of the CEP transactions, including transactions of events pre- processing. However, the propagation of these results for parallel event processing in loT is untimely.

A.K. Das , S. Zeadally , D. He et al. [3] presented a generalized taxonomy of various security protocols needed for the IoT environment. Their taxonomy included various important security services such as key management, user and device authentication, access control,

ISSN- 2394-5125 VOL 07, ISSUE 19, 2020

privacy preservation, and identity management. They also presented a detailed comparative analysis of recently proposed IoT-related state-of-art security protocols for various security and functionality features. Fur- thermore, they discussed various security challenges that need to be addressed to improve IoT security in the future.

Liu, X.; Trappe, W.; Lindqvist, J et.al [11] provided by network services is privacy protection, such as GNRS access control. The access control in the GNRS protects the data privacy, and also increases the difficulty of launching attacks by restricting adversarial access to information that is essential for launching an attack, whatever that attack might be. Access control enforced at the GNRS query is a powerful tool as it can provide the GNRS mapping owner, who is typically the data owner or a surrogate in the context of IoT, the ability of choosing who it is willing to communicate with. With the support of access control in the GNRS, IoT devices or data owners can protect the IoT data's location information contained in the GNRS mappings against unauthorized disclosure, while at the same time ensure the mapping's accessibility to legitimate subscribers or applications. In addition, GNRS access control can support advanced services, such as allowing the mapping owner to decide when and where it is reachable. These fine-grained functionalities provided by GNRS access control make it possible to specify detailed policies/regulations while distributing the data collected by the IoT devices.

III. Parallel Processing Of Multiple Levels Heterogeneous Data For End-To-End Collection And Analysis With Iot Security Using Novel Encrypted Code

The block diagram of parallel processing of multiple levels heterogeneous data for end-to-end collection and analysis with IoT security using novel encrypted code is represented in fig.1.

IoT Systems (Platforms & Devices) as this layer comprises the various elements of IoT systems that can act as sources of security information. The elements may be deployed on different IoT platforms and span multiple administrative domains.

Management and Configuration Tools module provides the means for managing and configuring the elements. In particular, it caters for the configuration of the probes and the registry, the management agents and their operation, as well as of the SPEP functionalities. Probes can be configured in terms of their deployment properties (e.g., where they reside), their data delivery rates, logging and data filtering, and so on. Likewise, the IoT probes registry can be configured in terms of the probes that are registered to it and their properties.

Management Agents is the security management agents provide the means for interacting with field IoT systems and devices for the purpose of implementing automation and actuation functions related to security. The deployment of management agents is similar to probes, yet there are differences in their functionality and operational characteristics, which led us to distinguish them from probes.

Visualization (Dashboards) provides a visualization of the status of the data collection and actuation layers. It is closely linked to the management and configuration functionalities so as to allow security operators and the administrators of the Secure IoT platform to visually manage the various components.

ISSN- 2394-5125 VOL 07, ISSUE 19, 2020

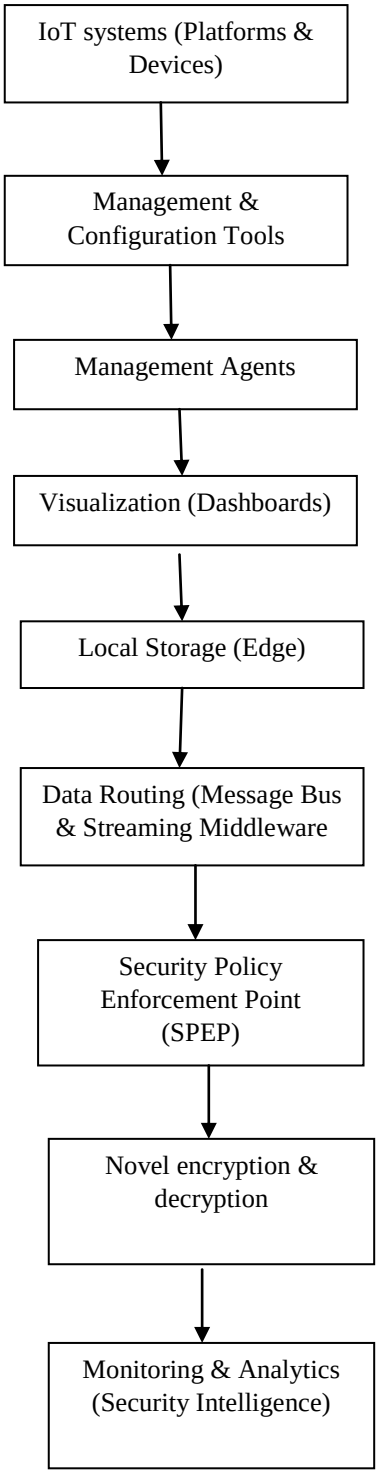

Fig.1: Block Diagram Of Parallel Processing Of Multiple Levels Heterogeneous Data For End-To-End Collection And Analysis With IoT Security Using Novel Encrypted Code.

Local storage refers to a local data store that provides persistence for the information that stems from the probes. It is characterized as "edge" or "local" data store as it is meant to store information close to the field and is distinguished from information that is stored at the cloud level. Local storage of security data can facilitate security intelligence based on edge analytics and edge intelligence, as a means of detecting and mitigating events at short/fine timescales. Note that the analysis of information at the local storage, may involve different types of analytics, but typically involves streaming analytics.

Data Routing is responsible for transferring security data from the probes to appropriate recipients / consumers of IoT security information. To this end, it interacts both with the registry for discovering and accessing the available probes and the data consumer components (i.e., security applications) that have appropriate permissions to access and process these data. The data routing component is typically implemented through a high-performance streaming middleware.

Security Policy Enforcement Point (SPEP) is the module that implements security policy enforcement decisions that are driven by analytics at the data collection and actuation layer or at the security intelligence layer. The latter decisions are of two main types: (i) Data collection configuration decisions that are targeted to the probes, and (ii) Security actuation and automation functionalities. SPEP plays an instrumental role on the intelligence and adaptive properties of the data collection process as it provides functionalities for changing the configuration and operation of the data collection in-line with the security context. Examples of SPEP functionality include the closing of a port, the disabling or enabling of certain functionalities of IoT components and so on. SPEP workflows can be described in a

high level policy description language (e.g., RuleML) or even in the form of Event-Condition-Action- Post-condition (ECAP) pipelines. Many IoT devices use symmetric encryption, in which **a** single key gets used to encrypt and decrypt data. The fact that the data gets encrypted offers a secure layer of security, particularly compared to using hardcoded or default passwords, but sharing and storing the encryption key creates risk.The data is monitored in monitoring and analytics.

IV. RESULT ANALYSIS

The result analysis of a parallel processing of multiple levels heterogeneous data for end-to-end collection and analysis with IoT security using novel encrypted code is demonstrated in this section. The security has improved in this model. The threats also reduced in this design.

The table 1 describes the performance analysis of the presented a parallel processing of multiple levels heterogeneous data for end-to-end collection and analysis with IoT security using novel encrypted code.

Table.1: Performance Analysis

Performance Analysis	Security	Threats
Data collection and analysis with IoT security using novel encrypted code	98	62
Data collection and analysis with IoT security using decrypted code	90	85

The above table shows that an the performance analysis of the presented parallel processing of multiple levels heterogeneous data for end-to-end collection and analysis with IoT security using novel encrypted code gives high security, and less threats.

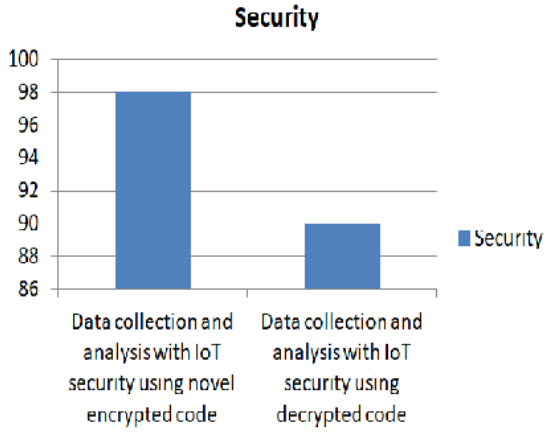

Fig.2: Security Comparison Graph

In Fig.2 security comparison graph the parallel processing of multiple levels heterogeneous data for end-to-end collection and analysis with IoT security using novel encrypted code shows higher security when compared with other models**.**

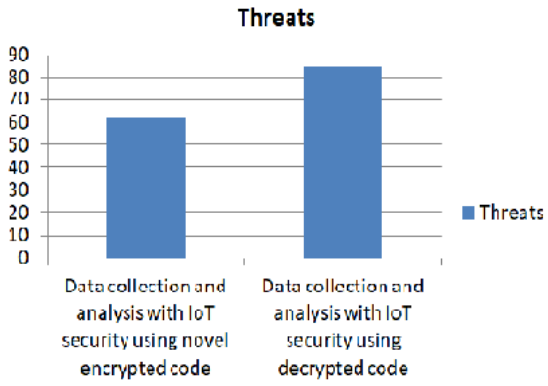

Fig.3: Threats Comparison Graph

Therefore in threats comparison graph shows less threats attacks for parallel processing of multiple levels heterogeneous data for end-to-end collection and analysis with IoT security using novel encrypted code when compared with the Data collection and

ISSN- 2394-5125 VOL 07, ISSUE 19, 2020

analysis with IoT security using decrypted code.

V. CONCLUSION

In parallel processing of multiple levels heterogeneous data for end-to-end collection and analysis with IoT security using novel encrypted code the approaches require collection and management of very large amounts of security data for training and building supervised and unsupervised learning systems that must be efficient and able to adapt to different security contexts and deployment configurations. It is therefore important to build scalable, extensible and well-designed infrastructures for collecting security data from all the different elements that comprise nontrivial systems including devices, edge/fog nodes and cloud computing infrastructures. This paper has shed light into the challenges of building such infrastructures. The presented solutions are configurable, scalable and intelligent, leveraging on existing BigData infrastructures. Hence, in this analysis the security is achieved and threats also decreased because of using novel encrypted code.

VI. REFERENCES

[1] U. Jayasinghe, G. M. Lee, T. Um and Q. Shi, "Machine Learning based Trust Computational Model for IoT Services", in IEEE Transactions on Sustainable Computing, May 2018.

[2] L. Xiao, X. Wan, X. Lu, Y. Zhang and D. Wu, "IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security?", in IEEE Signal Processing Magazine, vol. 35, no. 5, pp. 41–49, Sept. 2018.

[3] A.K. Das , S. Zeadally , D. He , Taxonomy and analysis of security protocols for internet of things, Future Gene. Comput. Syst. 89 (2018) 110–125 .

[4] J. Soldatos et al., "OpenIoT: Open Source Internet-of-Things in the Cloud", In: Podnar Žarko I., Pripužić K., Serrano M. (eds.) Interoperability and Open-Source Solutions for the Internet of Things. Lecture Notes in Computer Science, vol. 9001. Springer, Cham, Mar. 2015.

[5] M.-J. Kim and Y.-S. Yu, "Development of Real-time Big Da Analysis System and a Case Study on the Application of Information in a Medical Institution", Intern. Journal of Software Engineering and Its Applications, vol. 9, no. 7, 2015, pp. 93-102.

[6] N. Zygouras, N. Zacheilas, V. Kalogeraki, D. Kinane, and D. Gunopulos, "Insights on Scalable and Dynamic Traffic Management System", Proc. of the 18th Intern. Conference on Extending Database Technology (EDBT), 2015, pp. 653-664.

[7] N.P. Schultz-Meller, M. Migliavacca, and P. Pictzuch, "Distributed Complex Event Processing with Query Rewriting", Proc. of the Third ACM Intern. Conference on Distributed Event-Based Systems,

[8] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges," in Wireless Networks, Vol. 20, Issue 8, November 2014, pp. 2481-2501.

[9] H. Zhang, Y. Diao, N. Immerman, "On Optimization of Expensive Queries in Complex Event Processing", Proc. of the 2014 ACM SIGMOD Intern. Conference on Management of Data (SIGMOD '14), 2014, pp.217-228.

[10] D. Gyllstrom, E. Wu, H.-J. Chae, Y. Diao, P. Stahlberg, and G. Anderson, "SASE: Complex Event Processing over Streams", https://arxiv.org/ftp/es/papers/0612/0612128.pdf

[11] Liu, X.; Trappe, W.; Lindqvist, J. A Policy-driven Approach to Access Control in Future Internet Name Resolution Services. In Proceedings of the 9th ACM workshop on Mobility in the Evolving Internet Architecture, Maui, HI, USA, 7–11 September 2014; pp. 7–12.

[12] A. Moraru and D. Mladenić, "Complex Event Processing and Data Mining for Smart Cities", 15th International Multi conference on the Information Society, Ljubljana 2012, http://ailab.ijs.si/dunja/SiKDD2012/Papers/Moraru CEP.pdf.

[13] D. Anicic, S. Rudolph, P. Fodor, and N. Stojanovic, "Stream reasoning and complex event processing in ETALIS". Semantic Web. vol. 3, no. 4, pp. 397-407, 2012. DOI: 10.3233/SW-2011-0053.

[14] D. Wang, E.A. Rundensteiner, and R.T. Ellison III, "Active Complex Event Processing over Event Streams", Proc. of the VLDB Endowment, Vol. 4, no. 10. 2011.pp. 634–645.

[15] J. Hui and P. Thubert, "Compression format for IPv6 datagrams over IEEE 802.15. 4-based networks", Internet proposed standard, RFC 6282, 2011.

[16] L. Atzori , A. Iera , G. orabito , The Internet of Things: a survey, Comput. Netw. 54 (15) (2010) 2787–2805 .

[17] S. Tranchard, New ISO RFID standard will help trace products in the supply chain, 2010, http://www.iso.org/news/2010/02/Ref1293.html .

[18] Ken Bever, "The OpenO&M Information Service Bus and Common Interoperability Registry", October 2009.

[19] K. Ashton, "That 'internet of things' thing", *RFiD Journal*, vol. 22, no. 7, pp. 97-114, 2009.

[20] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, "Transmission of IPv6 packets over IEEE 802.15. 4 networks", 2070-1721, 2007.