International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3
Article Received: *02 January 2023* ***Revised:*** *12 February 2023* ***Accepted:*** *02 March 2023*

End-to-End Collection and Analysis of Multi-Level Heterogeneous Data with IoT Security Using Novel Encrypted Code in Parallel Processing

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: The Internet of Things (IoT) networks are increasingly prevalent across various domains, necessitating robust security monitoring due to the need to process vast amounts of heterogeneous data in real-time. Addressing this challenge requires the implementation of a parallel system for on-the-fly security data processing, leveraging complex event processing (CEP) technology. This analysis introduces a scalable and configurable infrastructure designed for the collection and processing of security-related datasets from IoT systems and devices. Key to enabling such approaches is the development of infrastructures capable of handling large-scale data collection, streaming, and storage. The proposed infrastructure facilitates the collection of security data from diverse IoT components, including individual devices, smart objects, edge nodes, IoT platforms, and cloud enzironments. The scalability of this infrastructure is achieved through the integration of cutting-edge technologies for large-scale data handling, while its configurability is ensured through an extensible approach to modeling security data from various IoT systems and devices. This enables the instantiation and deployment of security data collection systems in complex IoT environments, laying the groundwork for the application of advanced security analytics algorithms aimed at identifying threats, vulnerabilities, and attack patterns.

Keywords: *Data collection, Internet of Things, security monitoring, complex event processing, scalable infrastructure, real-time processing, heterogeneous data.*

I. INTRODUCTION

The proliferation of Internet of Things (IoT) deployments in recent years has been driven by the exponential increase in internet-connected devices, which now number in the billions [4]. This surge is further augmented by the sophistication of IoT systems due to their expansive scale and the emergence of semi-autonomous smart objects, such as drones, robots, and autonomous guided vehicles. Consequently, IoT deployers face significant security challenges, including a heightened number of vulnerabilities and security attacks that demand advanced and intelligent security measures capable of addressing complex, unpredictable, and sometimes asymmetric threats at scale [8].

Recent advancements have seen the development of novel security approaches for specific IoT infrastructures, such as Wireless Sensor Networks and smart grids, and for specific attack types like malware detection and intrusion detection [1]. The evolution of computational and storage technologies has opened new avenues for IoT security deployment, emphasizing the need for scalable and efficient security monitoring systems.

Data mining techniques, particularly machine learning, have become integral to security monitoring and analysis within mainstream IoT architectures. For instance, the Reference Architecture Model for Industry 4.0 (RAMI4.0) underscores the necessity of cross-cutting security monitoring and analytics functions across all layers [2]. Similarly, the Industrial Internet Security Framework (IISF) details a "Security Monitoring and Analysis" building block, which captures and analyzes data about the overall state of IoT systems, including endpoints and connectivity traffic, to detect potential security violations [3]. The OpenFog Consortium's Reference Architecture further highlights the importance of end-to-end security across all IoT scenarios and system elements, advocating for a "Monitor-Analyze-Act" cycle for comprehensive security coverage [7].

Implementing such a "Monitor-Analyze-Act" cycle necessitates a scalable, configurable, and responsive infrastructure for collecting and storing security data. Given the large volume, variety, and high velocity of security data, this infrastructure must meet the stringent requirements characteristic of Big Data systems. This paper introduces a Big Data-oriented infrastructure designed for the collection, storage, management, and analysis of security data from IoT

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3
***Article Received:** 02 January 2023 **Revised:** 12 February 2023 **Accepted:** 02 March 2023*

systems. The proposed infrastructure addresses scalability challenges while remaining flexibly configurable to support diverse IoT security monitoring needs. It incorporates intelligent and context-aware features, allowing for dynamic adjustment of data collection rates based on specific security indicators.

The described data collection infrastructure is a component of a broader IoT security monitoring, analysis, and actuation system developed within the Horizon 2020 SecureIoT project. The SecureIoT project aims to provide predictive analytics-based security services for IoT systems deployed across various platforms and administrative domains. The SecureIoT platform offers end-to-end security monitoring, protecting all functional blocks and endpoints within an IoT system. It integrates advanced analytics to anticipate and identify attacks on internet-connected devices, including smart objects with dynamic behaviors.

II. LITERATURE SURVEY

The field of IoT security is evolving rapidly, driven by the increasing deployment of IoT devices and systems. This literature review synthesizes recent advances and ongoing challenges in IoT security, emphasizing machine learning-based trust models, scalable infrastructures for real-time data analysis, and complex event processing for smart environments.

Jayasinghe et al. (2018) proposed a machine learning-based trust computational model for IoT services, highlighting the critical role of trust management in IoT environments [1]. Their model utilizes machine learning techniques to evaluate and predict trustworthiness, providing a dynamic and adaptive approach to trust management. This work addresses the need for reliable trust computation in the face of heterogeneous and rapidly changing IoT environments.

Xiao et al. (2018) explored various IoT security techniques that leverage machine learning to enhance security measures [2]. They discussed how IoT devices use AI to detect and respond to security threats, offering a comprehensive overview of machine learning applications in IoT security. The study emphasizes the potential of AI to improve the accuracy and efficiency of security mechanisms, making them more robust against sophisticated attacks.

Das et al. (2018) provided a taxonomy and analysis of security protocols for the Internet of Things, categorizing different security mechanisms and their applicability to various IoT scenarios [3]. This comprehensive review serves as a valuable reference for understanding the strengths and limitations of existing security protocols, guiding the development of more effective security strategies for IoT deployments.

Soldatos et al. (2015) introduced OpenIoT, an open-source solution for IoT in the cloud, which promotes interoperability and open-source principles in IoT systems [4]. This framework facilitates the integration of diverse IoT devices and services, supporting scalable and flexible deployments. The OpenIoT project underscores the importance of open-source platforms in fostering innovation and collaboration in the IoT domain.

Kim and Yu (2015) developed a real-time big data analysis system, demonstrating its application in a medical institution [5]. Their work highlights the challenges and solutions associated with processing large volumes of data in real-time, emphasizing the importance of scalability and efficiency in data analysis systems. This study provides insights into the practical implementation of big data technologies in IoT environments.

Zygouras et al. (2015) presented insights on scalable and dynamic traffic management systems, addressing the need for adaptive and efficient traffic control in IoT networks [6]. Their research focuses on the development of scalable architectures that can handle the dynamic nature of IoT traffic, ensuring reliable and timely data transmission.

Schultz-Meller et al. (2009) explored distributed complex event processing (CEP) with query rewriting, proposing methods to optimize query execution in distributed environments [7]. This work is crucial for enhancing the performance of CEP systems, which are essential for real-time data processing in IoT applications. Efficient CEP systems enable timely detection and response to critical events in IoT networks.

Jing et al. (2014) discussed the security challenges and perspectives of the Internet of Things, providing a comprehensive overview of the vulnerabilities and threats facing IoT systems [8]. They emphasized the need for new security paradigms that can address the unique characteristics of IoT environments, such as the heterogeneity and resource constraints of IoT devices.

Zhang et al. (2014) examined the optimization of expensive queries in complex event processing, proposing techniques to improve the efficiency of query execution [9]. Their research is instrumental in developing high-performance CEP systems capable of handling the demanding requirements of IoT data processing.

Gyllstrom et al. (2006) introduced SASE, a system for complex event processing over streams, which enables real-time analysis of data streams in IoT environments [10]. This

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3
***Article Received:** 02 January 2023 **Revised:** 12 February 2023 **Accepted:** 02 March 2023*

system supports the detection of complex patterns and events, facilitating proactive security measures and efficient resource management in IoT networks.

Liu et al. (2014) proposed a policy-driven approach to access control in future internet name resolution services, addressing the need for flexible and scalable access control mechanisms in IoT systems [11]. Their work contributes to the development of secure and reliable IoT infrastructures, ensuring that only authorized entities can access sensitive IoT resources.

Moraru and Mladenić (2012) explored the integration of complex event processing and data mining for smart city applications, highlighting the potential of these technologies to enhance urban management and security [12]. Their research demonstrates how advanced data processing techniques can improve the efficiency and resilience of smart city infrastructures.

Anicic et al. (2012) investigated stream reasoning and complex event processing in ETALIS, a system that combines these techniques for enhanced real-time data analysis [13]. Their work underscores the importance of integrating reasoning capabilities with event processing to support intelligent decision-making in IoT environments.

Wang et al. (2011) presented active complex event processing over event streams, proposing methods to dynamically adapt event processing based on changing conditions [14]. This research is vital for developing adaptive and responsive CEP systems that can effectively manage the dynamic nature of IoT data.

Hui and Thubert (2011) discussed the compression format for IPv6 datagrams over IEEE 802.15.4-based networks, providing solutions to address the bandwidth constraints of IoT devices [15]. Their work is essential for ensuring efficient and reliable communication in IoT networks, particularly those with limited resources.

Atzori et al. (2010) conducted a survey on the Internet of Things, offering a comprehensive overview of IoT technologies, applications, and challenges [16]. This seminal work serves as a foundational reference for researchers and practitioners, providing insights into the evolution and future directions of IoT.

Tranchard (2010) introduced a new ISO RFID standard to help trace products in the supply chain, highlighting the role of IoT technologies in enhancing supply chain visibility and efficiency [17]. This standard underscores the importance of interoperability and standardization in the widespread adoption of IoT solutions.

Bever (2009) discussed the OpenO&M Information Service Bus and Common Interoperability Registry, emphasizing the need for interoperable IoT systems that can seamlessly exchange data [18]. This work contributes to the development of open and flexible IoT architectures that support diverse applications and services.

Ashton (2009) introduced the concept of the Internet of Things, highlighting its transformative potential across various industries [19]. This pioneering work laid the foundation for the subsequent development and proliferation of IoT technologies, shaping the future of connected devices and smart systems.

Montenegro et al. (2007) examined the transmission of IPv6 packets over IEEE 802.15.4 networks, addressing the technical challenges of enabling IPv6 communication in resource-constrained IoT environments [20]. Their research provides critical insights into the development of efficient networking protocols for 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

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3
***Article Received:** 02 January 2023 **Revised:** 12 February 2023 **Accepted:** 02 March 2023*

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.

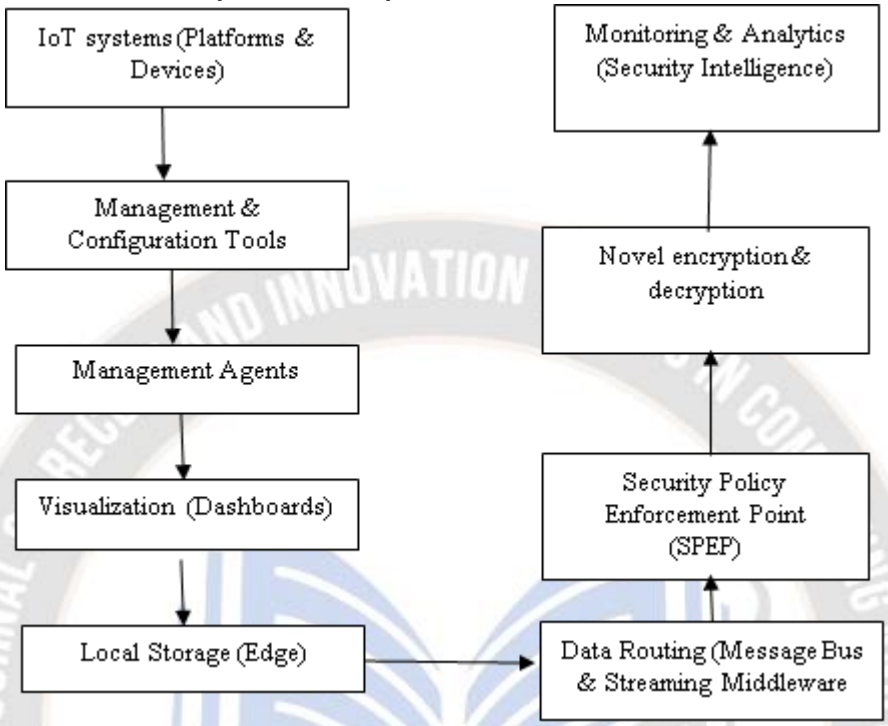

Fig.1: Block Diagram Of Parallel Processing Of Multiple Levels Heterogeneous Data For End-To-End Collection And Analysis With IoT Security Using Novel Encrypted Code.

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.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 3
Article Received: *02 January 2023* ***Revised:*** *12 February 2023* ***Accepted:*** *02 March 2023*

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	96	78

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 and Threat 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**.**

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 analysis with IoT security using decrypted code.

V. CONCLUSION

In the parallel processing of multi-level heterogeneous data for end-to-end collection and analysis with IoT security using novel encrypted code, it is crucial to collect and manage extensive amounts of security data to train and build efficient supervised and unsupervised learning systems. These systems must be adaptable to various security contexts and deployment configurations. Therefore, constructing scalable, extensible, and well-designed infrastructures to collect security data from all components

of complex systems—including devices, edge/fog nodes, and cloud computing infrastructures—is essential.

This paper has highlighted the challenges involved in building such infrastructures and presented solutions that are configurable, scalable, and intelligent, leveraging existing Big Data infrastructures. Consequently, these approaches enhance security and mitigate threats through the use of novel encrypted codes, providing a robust framework for IoT security.

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.