Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 175 (2020) 730–736

Procedia Computer Science

www.elsevier.com/locate/procedia

The 2nd International Workshop on Emerging Networks and Communications (IWENC 2020)
9-12 August 2020, Leuven, Belgium

Network Security Strategies in Big Data Context

Imane El Alaoui[a,*], Youssef Gahi[b]

[b]*LASTID, Laboratoire des Systèmes de Télécommunications et Ingénierie de la Décision, Ibn Tofail University, Kenitra, Morocco*
[a]*LGS, Laboratoire Génie des Systèmes, Ecole Nationale Sciences Appliquées, Ibn Tofail University, Kenitra, Morocco*

Abstract

Big data allows organizations to process massive and complex data to extract hidden patterns, draw insights, and also to share data through the network. Data that transit in an organization network is often sensitive and requires an efficient and secure platform. For this reason, network security has been brought to the forefront in the Big data era. In this context, network security platforms have to deal with vast and complex information to predict and prevent potential attacks in real-time. However, these platforms are often based on traditional approaches, which make them unreliable to secure big data. In this paper, we mainly focus on network security and protection strategies of big data. First, we highlight factors affecting network security platforms in the Big data era. Then, we go through different big data strategies that allow ensuring security across networks while surveying recent researches.

Keywords: Big Data, Network Security, Big Data challenges, Big Data strategies.

1. Introduction

The rapid growth and the extensive use of various emerging technologies, such as IoT, Cloud, 5G, social media,

* Corresponding author. Tel.: +212-537-329-246; fax: +212- 537- 329-24
E-mail address: imane.el.alaoui@uit.ac.ma

10.1016/j.procs.2020.07.108

co, and smart cities, lead to a vast, heterogeneous, and complex data, called big data. These data bring tremendous processing opportunities to various domains, including healthcare, politic, transport, and banking. It is essential to mention that big data also brings several challenges due to their complex characteristics, namely, Volume, Velocity, Variety, Veracity, Value, Variability, and Visualization, see Figure 1.

Big data technologies play a pivotal role in the process of collecting, analyzing, and visualizing massive and complex data. They help to discover hidden patterns and to extract useful and sensitive information. Big data technologies are continuously supporting powerful network platform aiming to interconnect data entities and share information across them. However, Big data is also an attractive zone for many security attacks that raise many challenges[1]. In fact, along with the high-speed growth of data that flows in networks, the network coverage scale is expanding, and the network environment is more complicated.

Further cyber-attacks are becoming increasingly prevalent and intricate. It is, therefore, imperative to use reliable and robust Network Security Platforms (NSPs) that provides high-performance reports in the real and near real-time. Nonetheless, traditional NSPs (TNSPs), like any conventional tool, are inadequate to detect attacks in large and complex data within a reasonable time. Effectively, Big data characteristics have a significant impact on NSPs, as summarized in Figure 1.

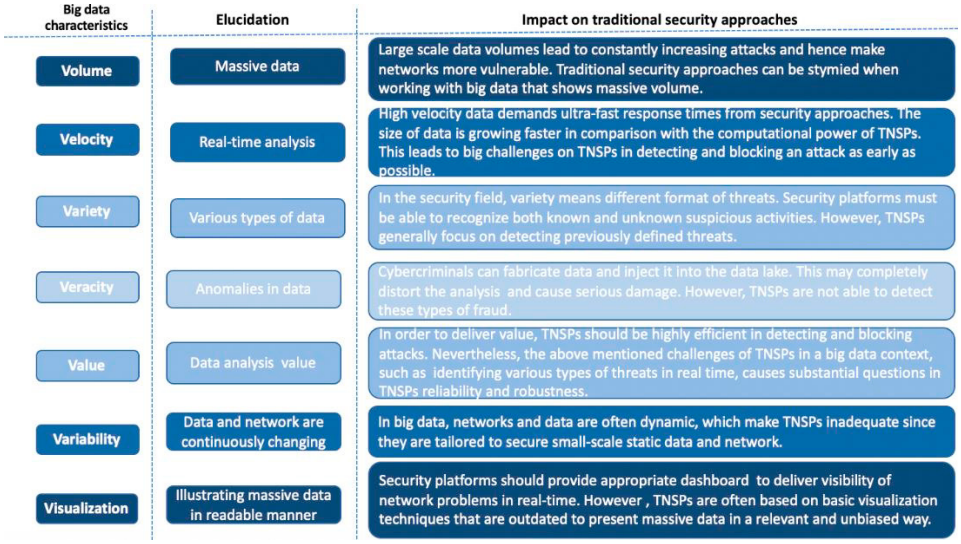

Fig.1 Network security risks in the Big data era

Considerable efforts have been made to reduce network security risk. However, as shown in the above figure, the complex nature of big data inhibits existing NSPs' performances in several levels, including real-time, accuracy, and reliability. Therefore, NSPs should attach great importance to Big data specificities to align as much as possible with the contexts implementing big data. This paper aims to provide big data strategies that should be considered in NSPs to align with Big data needs.

The rest of the paper is organized as follows: Section 2, 3, and 4 discuss big data strategies that allow NSPs to produce adequate security analytics in terms of managing big data through the network. Furthermore, we highlight recent and exciting contributions that have been proposed in this regard. Finally, Section 5 concludes the paper by giving some future directions.

2. Threat detection

Threat detection is a priority security solution that must be integrated even in primary security platforms. It is designed to detect and prevent malicious activities in the network. The idea is to detect threats before they are exploited as attacks, gain unauthorized access to internal systems, and cause damage. It plays a pivotal role in cyber-security, especially in the context of Big data. It allows protecting the confidentiality, integrity, and availability of Big data from advanced and persistent malware attacks in the network environment, see Figure 2.

To maintain the security of the network in the context of Big data, many researchers have provided efficient techniques based on Big data analytics and Artificial Intelligence (AI). For instance, Camacho et al. [2] have come up

with a Multivariate Big data Analysis, an intrusion detection approach that allows handling massive amounts of heterogeneous data sources. The proposed method is based on Multivariate Statistical Network Monitoring (MSNM) technique proposed in [3]. It allows not only to detect anomaly but also gives logs details about information corresponding to this anomaly. The experimental results have shown that this system identifies the raw information of the attack with high specificity, more than 99%.

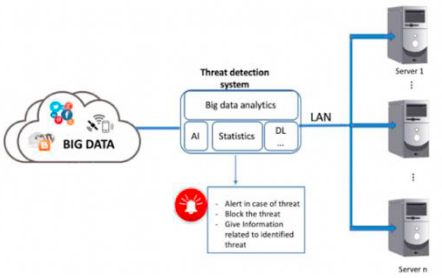

Fig.2 Threat detection

In [4], Yang et al. have designed a Big data analytics platform that not only detects anomalies that represent the performance degradation of a cellular network in wireless mobile networks but also perform a root cause analysis. First, the anomaly detection module is delivered by preprocessing data, applying a statistical model called Univariate Anomaly Detection, and finally, a post-processing filtering to remove false alarms. Then, the root cause analysis module is performed using an unusual association rule learning approach to quarry association between crucial quality indicators and critical performance indicators anomalies that occur infrequently.

Li and Min have proposed in [5] a marking method to improve network attack detection basing on Big data fusion tracking recognition. This technique allows classifying the data types of the network attack node. The simulation results have shown that the proposed method can effectively locate network attack nodes with an accuracy of 94%.

As mentioned above, it is challenging to express massive data accurately. It is also important to say that Deep Learning brings a new way to deal with Big data by automatically learning features[6]. Furthermore, DL allows getting more profound information than traditional methods. More and more researches put forward DL-based frameworks to ensure network security. In [7], Faker and Dogdu have combined Big data, Deep Feed-Forward Neural Network, and two ensemble techniques (RF and GBT) to enhance the performance of intrusion detection systems. The two ensemble techniques are implemented on Apache Spark, while the deep learning model is implemented using Keras. The experimentation results show that the proposed method achieves high performance, up to 99.99%. Another intrusion detection system using deep learning and Big data processing capabilities is introduced in [8]. Flume, Flink, and a deep learning algorithm called Auto-Encoder are used. The proposed approach has shown high performances, about 94.32% of accuracy. Other contributions have also offered attractive and efficient strategies to secure networks basing on different DL algorithms, such as LSTM [9].

3. Network security assessment

All the mentioned above contributions allow us to detect threats efficiently and comprehensively solve the security problem and do not consider the specificities of the used network. New approaches must, therefore, be proposed to ensure security basing on the security gaps of the studied system. The leading solution that allows bridging this gap is the network security assessment. It consists of auditing and evaluating the security quality and show where the fundamental weaknesses are. Network security assessment plays an essential role in network security due to its capability to increase system protection in depth. Effectively, such a risk assessment allows to identify vulnerabilities in different environment, measure the size of potential impacts of successful attacks, test the robustness of security defenders to detect and respond to attacks. Also, it locates any external or internal entry points in the network. Moreover, it prescribes the steps that should be taken to protect the possible attacks, basing on the identified weakness.

Several contributions have been proposed to evaluate the network security assessment based on Big data. Huang [10] has combined Big data modeling and statistical analysis to assess security and detect anomaly for campus network management. The statistical analysis, namely the fuzzy algorithm, is used to identify abnormal activities in the campus network. In contrast, Big data fusion is used to secure a quantitative assessment of network management security. The conducted experimentation shows that the proposed approach achieves good accuracy, up to 99,6%.

Always in the same context, Kim et al. [11] have proposed a Big data framework to strengthen network security in the context of SMEs (Small and Medium-sized enterprises). The proposed framework allows visualizing the security capability of SMEs via mobile devices. For this, several statistical analysis methods, such as linear regression and partial least squares, were used to diagnosis the security capability. Then, a solution is developed to improve the security capability basing on the diagnostic.

In [12], Lin and Chen have proposed a Network Security Situation Assessment System in Big data environment. The system protects the core information infrastructure in a large-scale network. First, the proposed model divides a massive network into multiple modules using the BGLL algorithm and preprocess data on Hadoop. Then, it evaluates the security of the nodes in each module basing on the SimHash algorithm. The module security situation is obtained according to the security situation of its related nodes, and finally, the network security situation is quantified using the combination of the weight and the security situation of the modules

Ye [13] has designed a new algorithm that assesses network intrusion risk under substantial intrusion interference. This algorithm is based on Big data association rule mining to judge the behavior characteristics of network intrusion association data. Then a stochastic linear fitting model is used to adjust the result to enhance the algorithm performances under substantial intrusion interference. The experimentation shows that the proposed algorithm achieves good accuracy (between 92% and 100%) in evaluating the regular data on network intrusion.

4. Scalability

With the increasing amount of large-scale data, the higher requirement regarding the speed of data analysis has been raised. It must be pointed out that traditional architecture, even a high-end one, is unable to process this large-scale data and provide a secure network. For this reason, new processing capabilities, called Big data tools, have emerged to help us cope with the scalability challenges of Big data[14]. These tools rest on distributed architecture to allow analysis, storage, and manipulation of large amounts of data in a reasonable time.

There are several potential benefits of the "scale-up" approaches, especially in network security. Security platforms should provide efficient access to information, high performance, and real-time queries. Hence, there is a growing need for scalable network security systems in the context of Big data, see Figure 3. In what follows, we discuss scalable analytics platforms designed for network security in the background on Big data.

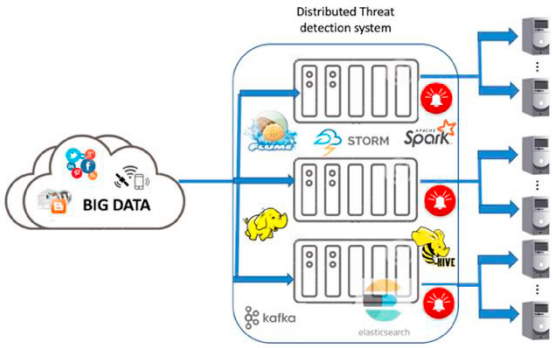

Fig.3 Scalable threat detection system

Sarlis et al. [15] have proposed a fast and scalable system for network monitoring and management, called Datix. This system is based on Big data technologies such as Hadoop, Hive, and Shark. Its main contribution is to realize efficiently distributed joins algorithms and filtering queries within a few minutes. For this aim, authors have introduced a pre-partitioning schema that accelerates the execution time by combining static and dynamic approaches. The static partitioning consists of using a uniform partition scheme in the join fields of the log dataset. In contrast, the proactive approach use K-dimensional Tree, a dynamic data structure to partition the dataset. The experimentation has shown that the proposed scheme reduces query execution time by 70% compared to the basic Hive and Shark.

Lv et al. [16] have designed a novel network monitoring system using Big data technologies, mainly ElasticSearch and Kibana. The system consists of four primary functions: collecting Netflow in real-time, transferring data reliably basing on Logstash, storing data in ElasticSearch, and finally, analyzing and displaying data in real-time with Kabana.

It has been experimentally demonstrated that the proposed system provides real-time control for large-scale network security.

Traditional scaled-out application is composed of several instances and a load balancer that dispatches incoming traffic between them often based on round-robin. Unlike these conventional methods, Frishman et al. [17] have proposed an exciting load balancing approach for security appliance using clustering. K-means is used to distribute groups of similar networks across the instances of network security platforms basing on several features such as destination, service, and domain expert. The experimentation has demonstrated that the proposed approach can be used to improve network intrusion detection systems.

Zhang et al.[18] have designed a security architecture that includes a scalable network anomaly detection module and security data platform. Basing on LSTM, the proposed HTTP anomaly detection module allows detecting network anomalies efficiently, with an accuracy of 97.4% and a detection rate of 98.1%. It is also important to point out that real-time detection is provided by the proposed architecture by using a Restful API approach, ElasticSearch, and RabbitMQ.

To detect intrusion in networks efficiently, Sahi and Mohapatra [19] have compared several machine learning methods on a scalable architecture. This architecture is based on several Big data tools, namely, Hadoop, Hive, Spark, and Mahout. The experimental results have shown that the highest accuracy is achieved by the KNN approach (up to 99.9%).

5. Dynamicity

In the context of Big data, networks are not only much larger but also become more complex and dynamic. However, the security network platforms mentioned above usually deal with a simple static network environment only and consider a restricted set of events and devices such as log management, intrusion, denial of service, and topology. Hence, they have limited capability to detect complex and dynamic attacks, especially in Big data, where networks' environments and configurations are continuously changing due to the add/on/off patterns of network connectivity. It is difficult to distinguish between a regular topology change and malicious behavior in a dynamic network environment. Furthermore, security platforms have varying posture changes concerning changes in the network. Conclusively, Yusuf et al. [20] have proved the effects of network changes on security metrics, such as risk and cost on attack paths, mode of attack path lengths, and shortest attack path, by analyzing simulations. The experimental analysis consists of observing security metrics in dynamic networks with several changes such as the emergence of new vulnerabilities without patching, the addition and removal of hosts, and the shift in firewall rules.

In this context of dynamicity, Lin and Chen [21] have proposed a dynamic Network Security Situation Prediction Method that not only quantifies the network security situation but also predict attack behavior in a dynamically changing network environment. This method is based on Big data technology and the Bayesian attack graph. Big data technology is used to fuse and preprocess, deduplication as well as useless data removing, network security situation factors. Then, a vulnerability prediction algorithm is used to predict the number of vulnerabilities in real-time. Finally, the new vulnerability is combined with the Bayesian attack graph to predict the attack path and its probability and assess the network security situation. The proposed model can accurately predict the attack behavior and quantify the network security situation, as shown in their experimentation.

Researchers in [22] have come up with a dynamic network anomaly detection system using deep learning. LSTM is used to classify anomalies in networks. An Attention Mechanism (AM) have been added to improve the performance of the model. The authors have also solved the class-imbalance problem in the CSE-CIC-2018 dataset by using an over-sampling algorithm called SMOTE. This algorithm allows for getting more samples for the small size classes to optimize the training process. To further optimize the model, they have also used Adam gradient descent method that calculates the gradient of the loss function and updates the model parameters to reach convergence. The overall performance of the proposed system reaches 96.2%, while the traditional LSTM achieves 93.33% in the conducted experimentation.

In [23], Liao et al. have proposed DNAV, anomaly analysis, and visualization tools for dynamic networks through spatiotemporal graph segmentation (e.g., time and locations of connectivity). In the conducted experimentation, authors have demonstrated the efficiency of the proposed tool in analyzing anomalies (identifying time and place of anomalous events) in nodes and edges in a dynamic network.

Other contributions, such as [24][25][26] have also designed security risk assessment systems for dynamic networks. However, there are still some limitations to these contributions in the context of Big data. They cannot deal with data streams with large-volume and velocity in real-time. This needs to be improved in the future to fit Big data requirements adequately.

6. Encryption

Data encryption is the process of transforming data from a readable format into the encoded form and can only be accessed by users with the correct decryption key. It could be an excellent complementary strategy in network security. It would allow assuring the preservation, confidentiality, and integrity of sensitive data that transit in the network (transmission and reception ends). In other words, data encryption could prevent attackers that access illegally to the system, from intercepting and stooling confidential information (Figure 4).

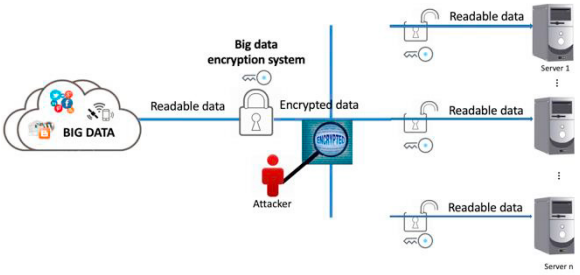

Fig.4 Network security basing on encryption

Many researchers are interested in this topic and provide interesting techniques to encrypt transited Big data. Wang [27] has proposed an iterative data encryption method to improve the security of transmission data anti-tampering in a supercomputer network, basing on elliptical, hyperbolic iterative coding. The tampering proof iteration is obtained using random quantitative coding fusion. Then, the logistics chaotic mapping system is used to realize the anti-tampering encryption, secure storage, and transmission in the network. The conducted experimentation has shown that the proposed scheme achieves excellent performance in terms of anti-attack and secure transfer of encrypted data.

To ensure end-to-end security and maintain confidentiality as well as the integrity for Big sensing data streams, Puthal et al. [28] have designed SEEN, a Selective Encryption method. It is based on a Data Stream Manager that allows us to perform intrusion detection and shared vital management. Moreover, SEEN allows adopting different keys, based on the data sensitivity levels, for three standards of data confidentiality, namely no confidentiality, partial confidentiality, and strong confidentiality. Theoretical analysis and experimental results have shown the efficiency of the proposed method in terms of processing time and assuring data confidentiality and integrity.

Hui and Zesong [29] have proposed not only an encryption method that improves the data transmission security, but also a prototype cluster that performs real-time analysis of log and network attack data. First, the model de-duplicate and standardize data to clean it. Then, the encryption method combines both ECC encryption and block encryption algorithms to ensure security and use a hybrid key generator based on semiconductor noise and chaotic sequence. This key generator is an efficient manner to build random keys that are hardly predictable, which enhances system security.

Other interesting encryption approaches have been proposed in [30][31][32]. They also allow effective content and structure protection against untrusted access and attacks.

7. Conclusion

Big data analytics is a burning topic that allows us to process and analyze large and complex data to discover hidden patterns. With the progress of big data analytics, network security became a relevant research field in the era of big data. It allows securing sensitive information that transits in the network. However, with the emergence of a large, heterogeneous, and complex data, existing security techniques become unable to process and identify threats in the network in a reasonable time. Furthermore, it often fails to provide adequate security analytics performance. In this

paper, we first show the impact of Big data specificities on network security. Then, we show some strategies that should be considered to build a reliable platform that deals with Big data issues.

As future work, we aim to design a network security system that fulfills all Big data requirements and considers the proposed strategies.

References

[1] Y. Gahi, M. Guennoun, and H. T. Mouftah, "Big Data Analytics: Security and privacy challenges," in *2016 IEEE Symposium on Computers and Communication (ISCC)*, Jun. 2016, pp. 952–957, doi: 10.1109/ISCC.2016.7543859.

[2] J. Camacho, J. M. García-Giménez, N. M. Fuentes-García, and G. Maciá-Fernández, "Multivariate Big Data Analysis for intrusion detection: 5 steps from the haystack to the needle," *Computers & Security*, vol. 87, p. 101603, Nov. 2019, doi: 10.1016/j.cose.2019.101603.

[3] J. Camacho, A. Pérez-Villegas, P. García-Teodoro, and G. Maciá-Fernández, "PCA-based multivariate statistical network monitoring for anomaly detection," *Computers & Security*, vol. 59, pp. 118–137, Jun. 2016, doi: 10.1016/j.cose.2016.02.008.

[4] K. Yang, R. Liu, Y. Sun, J. Yang, and X. Chen, "Deep Network Analyzer (DNA): A Big Data Analytics Platform for Cellular Networks," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 2019–2027, Dec. 2017, doi: 10.1109/JIOT.2016.2624761.

[5] P. Li and X.-C. Min, "Accurate Marking Method of Network Attacking Information Based on Big Data Analysis," in *2019 International Conference on Intelligent Transportation, Big Data Smart City (ICITBS)*, Jan. 2019, pp. 228–231, doi: 10.1109/ICITBS.2019.00061.

[6] Y. Gahi and I. El Alaoui, (in press), "Machine Learning and Deep Learning models for Big Data Issues," *Studies in Computational Intelligence*, 2020.

[7] O. Faker and E. Dogdu, "Intrusion Detection Using Big Data and Deep Learning Techniques," in *Proceedings of the 2019 ACM Southeast Conference*, Kennesaw, GA, USA, Apr. 2019, pp. 86–93, doi: 10.1145/3299815.3314439.

[8] Y. Dong, R. Wang, and J. He, "Real-Time Network Intrusion Detection System Based on Deep Learning," in *2019 IEEE 10th International Conference on Software Engineering and Service Science (ICSESS)*, Oct. 2019, pp. 1–4, doi: 10.1109/ICSESS47205.2019.9040718.

[9] A. Diro and N. Chilamkurti, "Leveraging LSTM Networks for Attack Detection in Fog-to-Things Communications," *IEEE Communications Magazine*, vol. 56, no. 9, pp. 124–130, Sep. 2018, doi: 10.1109/MCOM.2018.1701270.

[10] L. Huang, "Research on Campus Network Security Management Technology Based on Big Data," in *2019 International Conference on Smart Grid and Electrical Automation (ICSGEA)*, Aug. 2019, pp. 571–575, doi: 10.1109/ICSGEA.2019.00133.

[11] H.-K. Kim, W.-H. So, and S.-M. Je, "A big data framework for network security of small and medium enterprises for future computing," *J Supercomput*, vol. 75, no. 6, pp. 3334–3367, Jun. 2019, doi: 10.1007/s11227-019-02815-8.

[12] P. Lin, "Network Security Situation Assessment Based on Text SimHash in Big Data Environment.," *I. J. Network Security*, vol. 21, no. 4, pp. 699–708, 2019.

[13] Q. Y. Li, "Network Intrusion Risk Assessment Based on Big Data," in *2019 International Conference on Intelligent Transportation, Big Data Smart City (ICITBS)*, Jan. 2019, pp. 195–198, doi: 10.1109/ICITBS.2019.00053.

[14] I. El Alaoui, Y. Gahi, R. Messoussi, A. Todoskoff, and A. Kobi, "Big Data Analytics: A Comparison of Tools and Applications," in *Innovations in Smart Cities and Applications*, Cham, 2018, pp. 587–601, doi: 10.1007/978-3-319-74500-8_54.

[15] D. Sarlis, N. Papailiou, I. Konstantinou, G. Smaragdakis, and N. Koziris, "Datix: A System for Scalable Network Analytics," *ACM SIGCOMM Computer Communication Review*, 2015, doi: 10.1145/2831347.2831351.

[16] B. Lv, X. Yu, G. Xu, Q. Yin, and Z. Shi, "Network Traffic Monitoring System Based on Big Data Technology," in *Proceedings of the 2018 International Conference on Big Data and Computing*, Shenzhen, China, Apr. 2018, pp. 27–32, doi: 10.1145/3220199.3220221.

[17] G. Frishman, Y. Ben-Itzhak, and O. Margalit, "Cluster-Based Load Balancing for Better Network Security," in *Proceedings of the Workshop on Big Data Analytics and Machine Learning for Data Communication Networks*, Los Angeles, CA, USA, Aug. 2017, pp. 7–12, doi: 10.1145/3098593.3098595.

[18] G. Zhang, X. Qiu, and Y. Gao, "Software Defined Security Architecture with Deep Learning-Based Network Anomaly Detection Module," in *2019 IEEE 11th International Conference on Communication Software and Networks (ICCSN)*, Jun. 2019, pp. 784–788, doi: 10.1109/ICCSN.2019.8905304.

[19] S. K. Sahu and D. P. Mohapatra, "A Review on Scalable Learning Approches on Intrusion Detection Dataset," in *Proceedings of ICRIC 2019*, Cham, 2020, pp. 699–714, doi: 10.1007/978-3-030-29407-6_50.

[20] S. E. Yusuf, M. Ge, J. B. Hong, H. Alzaid, and D. S. Kim, "Evaluating the Effectiveness of Security Metrics for Dynamic Networks," in *2017 IEEE Trustcom/BigDataSE/ICESS*, Aug. 2017, pp. 277–284, doi: 10.1109/Trustcom/BigDataSE/ICESS.2017.248.

[21] P. Lin and Y. Chen, "Dynamic Network Security Situation Prediction based on Bayesian Attack Graph and Big Data," in *2018 IEEE 4th Information Technology and Mechatronics Engineering Conference (ITOEC)*, Dec. 2018, pp. 992–998, doi: 10.1109/ITOEC.2018.8740765.

[22] P. Lin, K. Ye, and C.-Z. Xu, "Dynamic Network Anomaly Detection System by Using Deep Learning Techniques," in *Cloud Computing – CLOUD 2019*, Cham, 2019, pp. 161–176, doi: 10.1007/978-3-030-23502-4_12.

[23] Q. Liao, T. Li, and B. A. Blakely, "Anomaly analysis and visualization for dynamic networks through spatiotemporal graph segmentations," *Journal of Network and Computer Applications*, vol. 124, pp. 63–79, Dec. 2018, doi: 10.1016/j.jnca.2018.09.016.

[24] J. B. Hong, S. E. Yusuf, D. S. Kim, and K. M. Khan, "Stateless Security Risk Assessment for Dynamic Networks," in *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*, Jun. 2018, pp. 65–66, doi: 10.1109/DSN-W.2018.00032.

[25] J. Wang, K. Fan, W. Mo, and D. Xu, "A Method for Information Security Risk Assessment Based on the Dynamic Bayesian Network," in *2016 International Conference on Networking and Network Applications (NaNA)*, Jul. 2016, pp. 279–283, doi: 10.1109/NaNA.2016.50.

[26] S. Yusuf Enoch, J. B. Hong, and D. S. Kim, "Time Independent Security Analysis for Dynamic Networks Using Graphical Security Models," in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, Aug. 2018, pp. 588–595, doi: 10.1109/TrustCom/BigDataSE.2018.00089.

[27] R. Wang, "Iterative Encryption Method of Transmission Data Anti-Tampering Based on Big Data," in *2019 International Conference on Virtual Reality and Intelligent Systems (ICVRIS)*, Sep. 2019, pp. 109–112, doi: 10.1109/ICVRIS.2019.00036.

[28] D. Puthal, X. Wu, N. Surya, R. Ranjan, and J. Chen, "SEEN: A Selective Encryption Method to Ensure Confidentiality for Big Sensing Data Streams," *IEEE Transactions on Big Data*, vol. 5, no. 3, pp. 379–392, Sep. 2019, doi: 10.1109/TBDATA.2017.2702172.

[29] Y. Hui and L. Zesong, "Research on Real-time Analysis and Hybrid Encryption of Big Data," in *2019 2nd International Conference on Artificial Intelligence and Big Data (ICAIBD)*, May 2019, pp. 52–55, doi: 10.1109/ICAIBD.2019.8836992.

[30] M. Islam, N. Nurain, M. Kaykobad, S. Chellappan, and A. B. M. A. A. Islam, "HEliOS: huffman coding based lightweight encryption scheme for data transmission," in *Proceedings of the 16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, Houston, Texas, Nov. 2019, pp. 70–79, doi: 10.1145/3360774.3360829.

[31] H. Shafagh, A. Hithnawi, L. Burkhalter, P. Fischli, and S. Duquennoy, "Secure Sharing of Partially Homomorphic Encrypted IoT Data," in *Proceedings of the 15th ACM Conference on Embedded Network Sensor Systems*, Delft, Netherlands, Nov. 2017, pp. 1–14, doi: 10.1145/3131672.3131697.

[32] C. Tschudin, "End-to-end encrypted scalable abstract data types over ICN," in *Proceedings of the 5th ACM Conference on Information-Centric Networking*, Boston, Massachusetts, Sep. 2018, pp. 88–94, doi: 10.1145/3267955.3267962.