NextGen Scientific Publication
American International Journal of Computer Science and Technology
Volume 5 Issue 5, Pg. No. 72-78, AIJCST-V5I5P107, 2023
https://doi.org/10.63282/3117-5481/AIJCST-V5I5P107

Original Article

An Algorithmic Baseline for Temporal Telemetry Anomaly Detection in Enterprise Cloud Architectures

***Mohammed Saad Javeed**
Trine University, 1 University Ave, Angola, IN, United States.

Abstract:

Cloud architectures are increasingly complex, and an effective anomaly detection is needed to detect abnormal behaviours from a flux of network telemetry data that are constantly produced in enterprises. The concept of this paper is to detect the temporal telemetry anomalies with basic idea of algorithmic baseline with the sequential cloud security data analysis using Long Short-Term Memory (LSTM) network. The proposed framework aims to monitor temporal dynamics of API-driven network telemetry, look for changes in traffic behavior, and surface possible security anomalies in the context of API vulnerabilities in Dynamic IP Address Management (IPAM). The idea behind it is to leverage on existing telemetry sequences learning to know what is normal and utilizing Mean Absolute Error (MAE) as an indicator of prediction error and as an anomaly detection method. Moreover, its architecture designs follow the sequential principles of Cloud security – mapped to the Zero Trust Architecture (ZTA) principles as mapped by NIST SP 800-207 – Continuous monitoring and Contextual verification and adaptive threat visibility and verification. It is proposed to create a baseline containing sufficient information to model and analyse Telemetry and for security based anomaly analysis of any suspicious activity in the network across time both in a dynamic enterprise cloud environment. The aim of the project is to develop an algorithmic solution to contribute positive to the monitoring of cloud infrastructures, reducing the obscurity of anomalies and proactively assess cloud security actions for the changing, distributed and modular constructions.

Keywords:

Long Short-Term Memory (Lstm), Temporal Telemetry Analytics, Dynamic Ip Address Management (Ipam) Vulnerabilities, Sequential Cloud Security, Nist Sp 800-207 Zero Trust Architecture, Mean Absolute Error (Mae), Api-Driven Network Telemetry.

Article History:

Received: 16.08.2023

Revised: 14.09.2023

Accepted: 26.09.2023

Published: 01.10.2023

1. Introduction

By this time, organizations have already embraced enterprise cloud vision and revolutionized the way they are managing their computing, network, and distributed applications. Application and services are becoming more interconnected and dependent on each other and now rely on application programming interfaces (APIs), virtual networks and dynamically allocated IP addresses, which allow scalable and flexible application behavior in cloud environments. All of these make the network more efficient and use resources more, but also raise security concerns with constantly changing network configurations, communication patterns and traffic behaviour. Most traditional methods to monitor the security of a temporal network rely only on comparing the behavior of the network at a certain point in time to some threshold and/or some rules of thumb and cannot easily detect subtle changes. Along with

Copyright by the Author(s). This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International (CC BY-NC-ND 4.0) License (https://creativecommons.org/licenses/by-sa/4.0/)

algorithmic anomaly detection, intelligent analysis of data collected via telemetry has now become critical to gain better visibility and strengthen security monitoring, especially in an enterprise cloud infrastructure.

A vast volume of data – operational and security – is created when network devices, virtual machines, application services, authentication systems and APIs interact and communicate with each other and this data needs to be retained and stored in the cloud. The analysis of these data streams is critical to detect abnormal communication patterns, and/or security breaches, and these should be done in as effective and efficient a way as possible. Their research sets a starting point for taking into account approaches for adaptive learning for Cloud based security systems. Similarly, Ahmad et al. [2] provided a comprehensive review of the security threats in IoT enabled-Cloud Computing which emphasized the challenges of Interconnected Devices, Cloud Computing and Distributed Communication.

In the study Kiani et al. [3] investigated the potential of classification of the possible transition from one of the multiple anomaly classes through neural network improvement. Their research has led them to identify the importance of this method in classification of complex abnormal pattern, with the aid of neural network. A similar functionality might be utilized in enterprise cloud systems to detect anomalous activities on network settings, instead of observing single pieces of telemetry data independently. A temporal analysis model that would analyze all the network activities over a period of time is more relevant as all the security anomaly can be easily detected by this type of analysis.

The protection of enterprise cloud architectures isn't only about any specific incident that happens on the network, but also has to include the identification and protection of important digital assets. Corrado et al. [4] proposed to classify critical assets and business impacts in an Industry 4.0 cyber security scenario. They serve as an example of the importance and necessity of understanding the relationship between innovation resources, functional dependence and cyber risks. Network telemetry gives essential details into interaction with communications, service dependence and interactions with resources in distributed cloud infrastructures. By monitoring these activities, it's possible to detect any abnormal activity in the network which could impact enterprise services available, integrity and confidentiality. Therefore, two concepts, namely pattern and security meaning need to be considered by anomaly detection mechanisms for temporal networks.

Another important component of telemetry-driven security analytics solutions are network traffic classification. Diverse traffic from APIs, application services, virtual machines and other components on the network flow through enterprise cloud infrastructure. However, effective methods of traffic representation and also a method of classifying normal traffic with possibly suspicious traffic are necessary. Telikani et al. [5] concentrates on analyzing cost sensitivity Network Traffic classification using deep learning based method and about the deployment of deep learning in understanding complicated network communication pattern. Their work helps give background for (possible) work on applying the learning based methods to cloud telemetry monitoring, in case the various services have different traffic but above all, if they are in different operational conditions. A classification differs in the sense that it is meant to give information about the kind of traffic it refers to, as temporal anomaly detection is about anomalies with respect to the expected sequential behaviour.

This paper aims to overcome the above problems by presenting an algorithmic pillars for temporal telemetry anomaly detection in Enterprise Cloud architecture leveraged by Long Short-Term Memory (LSTM) networks. What the authors put forward is to learn these sequential relationships of API based network telemetry, and use it to model the normal network behaviour to baseline. Temporal modelling with LSTM is believed to be appropriate for this, as it is able to perceive the dependence among successive observations, and analyse changing network patterns. Other areas highlighted by the framework are the Dynamic IP Address Management (IPAM) vulnerabilities: These will be conditions where the allocation/reassignment/include communication behavior is not an expected event, but may be a sign of a security vulnerability. Also added is the prediction deviation measure - the Mean Absolute Error (MAE) - which is useful to identify observations on telemetry with an error larger than the norm behaviour. Anomaly assessment process is an extension of the continuous monitoring and contextual verification processes of NIST SP 800-207 Zero Trust Architecture.

This research aims to build a structured algorithmic base to map temporal telemetry modelling, sequential anomaly identification and cloud security monitoring. New idea: Rather than “just” telemetry for the network, concentrate on analysing behaviour change over time. It's designed to present a starting point baseline framework for abnormal communication pattern identification, potential examination of vulnerabilities related to IPAM and support for security-oriented assessment in dynamic,

enterprise-level, cloud environments. The study therefore aggregates an all-encompassing conceptual and algorithmic perspective for telemetry analysis using LSTM, anomaly assessment based on MAE and Zero Trust oriented cloud security monitoring.

2. Related Work

Cloud security study and clever anomaly detection till now have been constrained to just apply machine learning that can discover uncommon actions in interconnected computing environment. Network telemetry grows and possibly gets more complex because of the emergence of cloud computing, IoT applications and API-driven infrastructure. Several studies are carried out on Cloud Data protection, Cloud Cyber Security threats, Anomaly Detection, neural networks and Network Traffic Classification, Intrusion Detection. The basis for the design of temporal telemetry analytics in enterprise cloud architectures are these contributions.

Mohiyuddin et al., [1] conducted a study on the secure Cloud storage of medical IoT data with the use of Adaptive Neuro-Fuzzy Inference System. The papers highlight the importance of the intelligent computational methods being used to protect sensitive information in cloud environments. Adaptive learning (mechanisms) is represented by an exemplary application of the use of the computational intelligence in decisions taking of distributed infrastructures, with security requirement support. They focus on secure storage of medical information; however for the present study their work is relevant in the context of usage of intelligent models with cloud computing security issues. Ahmad et al., in this article [2] give a detailed state of the art of cyber security in IoT based cloud computing and highlight the various cyber security problems and cyber security requirements of the connected IoT devices and cloud based platform. They present an overview of the security issues that the IoT networks and cloud creates in their study. All these are issues in enterprise set-ups where continually changing telemetry is generated by dynamically changing IPs, network set-up and APIs being called.

Corallo et al. [4] covered the topic of cybersecurity in the Industry 4.0 context, organising the answer in relation with a description of the criticality of the assets and the business impact. They learn about cyber security risk - critical digital assets – impact on Organisation. This holds true for cloud based systems too since changes to assets could be caused by problems on network resources, due to their unavailability or takeover of system components which depend on each other in relation with telemetry changes.

Another key stepping stone for security analytics based on telemetry is network traffic classification. Telikani et al. have introduced the concept of a cost sensitive deep learning approach for network traffic classification in [5]. In their result, they demonstrate the degree, to which deep learning can be used to analyze network traffic in terms of importance of classification results. In a like manner, Pant et al [6] proposed a 'Gated Recurrent Unit' (GRU) for detecting and identification of distributed denial of service (DDOS) attack. Applications of recurrent NN in Network Security Applications where Modeling of Sequential information is important. Mittal et al. [7] examined the techniques of neural network and GRU in intrusion detection and energy efficient route discovery.

The same can be applied to the field of enterprise telemetry; here, various traffic types also originate from cloud servers, and must be classified and monitored as well. Some other ML based approaches for IDS are looked at. Verma and Ranga [11] talked about the role of data driven techniques for detection of the malicious network activities and presented the machine learning based intrusion detection system for IoT applications. To solve the problems of network intrusion detection with the aid of deep learning, Khan et al. [12] provided two stage intrusive detection model. Djenouri et al. [13] discussed the issue of adapting nearest neighbours approach to detect spatio-temporal traffic flow anomalies. Their work is impactful to temporal analytics, because they consider both temporal and spatial aspects to detect deviations in the traffic behaviour. Hence this paper proposed a software-defined networking (SDN) based intrusion detection (IDS) from the generated datasets namely "INSDN" by Elsayed et al. [14] The results of their research illustrates the need for organized network data to develop and validate solutions for security analytics.

Finally, in Gill et al. [15] the future prospects and various increasing research areas based on artificial intelligence for the next generation computing has been discussed. Their studies broaden their perspective of the meaning of AIs well beyond on to Intelligent and Distributed Computing.

3. Zero Trust-Aware Temporal Telemetry Intelligence Framework for Enterprise Cloud Anomaly Detection

The suggested solution is discussed through an algorithmic solution, detecting abnormal behavioural patterns in enterprise cloud architectures, through analysis of temporal telemetry. It captures the telemetry data from the network API and conducts APIs

monitoring – monitors the dynamic IP address management (IPAM) before going on to carry out learning with the LSTM and deviation analysis with the MAE. The framework is conceptualized to look for the generation of network activity as well as to acknowledge activity that is not normally regarded as a kind of network activity. The principles and ideas to support continuous monitoring, contextual verification, and risk-aware interpretation of telemetry events are in NIST SP 800-207 Zero Trust principles. The framework is designed to allow proactive security monitoring in distributed cloud environments as it does not require a stable network configuration or access conditions. Figure 1 presents the proposed Zero Trust-aware temporal telemetry intelligence framework, illustrating the integration of cloud telemetry acquisition, sequential behavioural modelling, anomaly identification, and security assessment

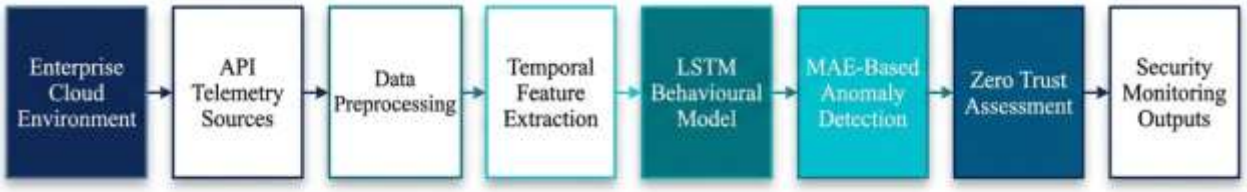


Figure 1. Zero Trust-Aware Temporal Telemetry Intelligence Framework

3.1. Architectural Overview and Functional Layers

These layers are six functional inter-indigenous layers that will be: Acquisition of the telemetry data, Pre-processing of the telemetry data, Represent the data to model its behaviours (with LSTM), Anomaly identification in each modelled behaviour, Implementation of Zero Trust approach for security assessment. For each layer a particular analytical problem is assigned to a certain analytical function specific to the particular problem and which serves as the input for the next layer. A multi-layer architecture enables the processing of the network observations and gives the ability to link single telemetry moments to a bigger series of telemetry moments.

The telemetry acquisition layer is used to collect information from the enterprise cloud infrastructure, as well as by using available APIs and/or network monitoring interfaces. These include changes of configurations or cloud, network flows information, communication records of services, allocation of some IP's, API usage records, etc. These sources give details on network identity, interactions with resources and communications etc. The acquisition layer provides all of the telemetry observations into a continuous stream of information which can be organised for time series information later analysis. It has no preference with one cloud supplier over other providers of cloud services, but favours availability and consistency of the telemetry.

3.2. API-Driven Telemetry Acquisition and IPAM Contextualization

Structured data from sites on the cloud can be acquired via API and shared with the framework. Figure 2 illustrates the telemetry acquisition and contextualization process through which API records, network events, and dynamic IPAM information are organized into a unified monitoring stream

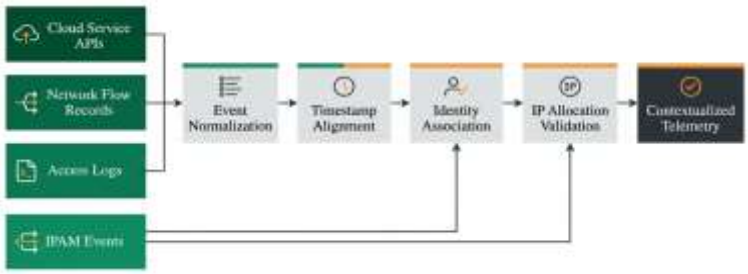


Figure 2. API-Driven Telemetry Acquisition and Dynamic IPAM Contextualization

3.3. Telemetry Preprocessing and Temporal Feature Representation

The data collected from the telemetry is analysed in a way that a coherent representation for a sequential analysis is produced. At this stage, schema deviations (data types) are processed in the cloud and time series data per service are processed too. The pre-

processing tasks consist of event normalization, event time bonding, duplicate-event elimination from observations, dealing with missing values and also organizing the sequence of the observations in the time ordered sequence. The operations are employed to present the input in an appropriate form for the learning component.

Available attributes of the telemetry are used to illustrate temporal features as changes in behaviour of cloud network. For example, this can include (but is not limited to) the frequency of communications, time of communication, pattern or change in API requests, access attempts, IP allocations, or service interactions, or pattern or change in network activity. The several features that can be measured in the working system characteristics of the monitored environment are selected depending on the significance. The issue with the framework is that it doesn't look at any particular individual that needs to be considered apart from other persons, but at the correlation of the time of the observation. This can help in the subsequent modelling of the behaviour of the network and if the behaviour of a specific event is an important deviation from the behaviour of the previous events.

3.4. LSTM-Based Sequential Behavioural Modelling

The recurrent architecture of LSTM is well suited for this framework as it incorporates memory mechanisms which help in representing relations between observations that occur at different time steps. Security behaviour of actions that can be important in enterprise cloud environments could involve a sequence of events, instead of single events. This may include API request failures, attempted access by unreliable/subversive IPs, unusual time/date stamps when API start or end interfaces change, unusual IP address reassignment, to name a few. It is shown in figure 3.

The temporally ordered feature sequences are then fed to the LSTM block where it is learnt to normal feature characteristics of behaviour. These it can control the retention and updating of the sequential information, picturing relevant temporal patterns, through controlling the content of its memory cells and gating mechanisms.

Modelling process may be proposed in 2 conceptual stages: Learning baseline, assessing the subsequent sequence. Baseline Learning: Learning from the past history with the help of telemetry data for the characterisation of the expected operational behaviour (Baseline Data). Sequences received are evaluated afterwards based on the learned behavioural representation. The deviation analysis part can then be used to look at changes in temporal attributes of the observations

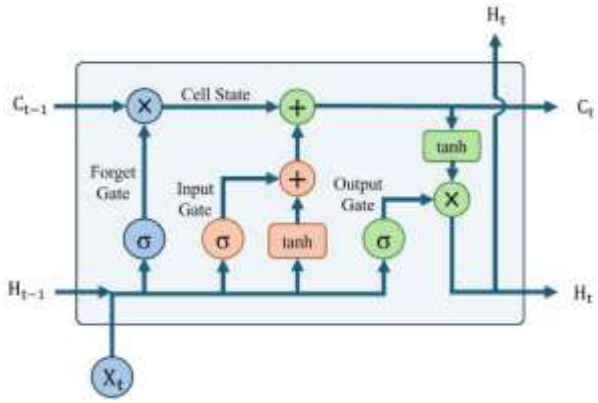


Figure 3. LSTM-Based Temporal Behavioural Learning Architecture

3.5. MAE-Based Deviation Analysis and Anomaly Identification

The proposed framework suggests the principal deviation measure of Mean Absolute Error. Finally, this process of modelling by means of LSTM leads to certain values (or behavioural representations) in expectation, which can then be compared to other similar observed values (e.g. telemetry). The MAE is the mean of the absolute errors of the predicted and the observed values. Deviation info is then used to alert the out-of-trend telemetry when compared to the healthy reference.

The anomaly Identification is the identification (assessment, comprehension) of the anomaly in terms of the associated telemetry parameter, and in operational environment. Deviation identified must be understood in the context of other factors and, subsequently, a security evaluation should be performed.

3.6. Zero Trust-Oriented Security Assessment and Monitoring Outputs

Finally, Zero Trust interpretation of deviations is based on the NIST SP 800-207 model of interpreting deviations from a security perspective. The design is based on the Continuous Verification – and the Contextual Access and Least Privilege Thinking. The machine that performs the analyse of the telemetry anomaly is correlated with the information available for service identity, access context, sensitivity of the resources as well as for the IPAM change.

Anomaly indications, deviations, summarized and related telemetry attributes and security assessment records are all examples of types of monitoring output. These outputs will give you information, which can be utilized for additional investigations by cloud administrators and security teams.

4. Operational Empirical Assessment of Temporal Telemetry Intelligence and Zero Trust Alignment

Issues such as time of validity of the telemetry, dynamic handling of an IP address, sequential inquiry and Zero Trust security needs are being addressed and examined within the framework of the proposed architecture. Evaluate the following aspects if realistic basis and relevant involving the components of the framework: It gives no indication of any experiment measurement, nor is it meant to promise in terms of largeness of performance, but rather simply assess whether or not the proposed architecture will allow the monitoring and security needs stated to be found can be met.

4.1. Assessment of Telemetry Acquisition and Operational Relevance

For the distributed cloud, a data acquisition layer driven by API is crucial to provide a foundation for monitoring.

4.2. Assessment of Temporal Modelling and Behavioural Representation

This indicates the sensible approach of this framework to store the baseline-learning paradigm also and compare it later with deviations. Its analytical value will be dependent on representativeness of historical telemetry, however. If the makeup of the workload changes in an interesting way (such as a new set of stats is applied to a baseline where users are NOT in the workload), then perhaps a special set of stats should be applied to a new baseline so that the alarm is not working on stats from users who aren't in the workload.

4.3. Assessment of Dynamic IPAM Vulnerability Context

Important because suspicious activity can't be noticed from an address change alone that is put into the context. If an unusual level of API access or communications activity had been expected it might possibly be an actual move or a reassignment, and would warrant further investigation; if it was a reassignment into an authorized infrastructure, it might have been an expected event. The second advantage of the proposed integration is the enhanced meaningfulness of the interpretation of the telemetry data, and a consistent change of the network identity corresponds to events that lead to a change in the operation of the network.

4.4. Assessment of MAE-Based Anomaly Identification

It is simply possible to compare the difference between the data predicted and observed telemetry data by using MAE. It is open to interpretation, and so can be used to determine deviations between the selected behavioural features. Deviation threshold should however be determined with regard to the following points: Monitored environment characteristics and individual telemetry attributes sensitivity. Keys can be more than one barrier to the different cloud services and workloads. In addition, in cases where the rate of deviations is high, it is not necessarily a security incident. The framework thus takes into account MAE as an anomaly and not just one mechanism to find out which is malicious activity.

4.5. Zero Trust Alignment and Overall Framework Suitability

just the location of the network. The framework is therefore conceptually and practically suitable to structure temporal telemetry analysis of enterprise cloud architectures to date. It works in a sequential behavioural modeling, dynamic IPAM context with deviation based anomaly identification, which are the key strength. Its use in practise will only be successful depending on the quality of the telemetry, baseline maintenance, the policies it establishes in the scope of its operation and of course empirical evaluation in actual cloud scenarios.

5. Conclusion

This is because it introduces a requirement that a set of behaviours occurring within a cloud network must be considered as a set of correlated behaviours, and not merely as a series of observations – this provides a baseline algorithmic approach to temporal anomaly detection, as opposed to the traditional approach of simply using LSTM-based sequence-modeling algorithm, in conjunction

with API-based telemetry, and deviation/Contextualization of the temporal data through dynamic IP address management (IPAM). It aggregates all the telemetry data from API calls and conversations in the network, access events and IP address allocation and then displays it in a structured format to make understanding the evolving situation of an operation more straightforward. LSTM incorporates the idea of concept mechanism that learns the temporal relations, and models in cloud the normal behaviours properties of the environment. Based on the analysis using MAE, it is possible to detect discrepancies set of predicted patterns of telemetry and set of observed pieces of telemetry while discrepancies of IPAM event context could be leveraged to classify the context as legitimate (infrastructure modifications) or suspicious. The framework notes as a side note that any "all deviations" is not necessarily a security incident.

Rather, it resonates with the context of the operation and the Zero Trust of NIST SP800-207 and a reminder of the need to continually verify and context of access. Ingesting temporal analytics and dynamic network identity planning in an integrated way in a single cloud monitoring paradigm has Zero Trust boundaries and is the major benefit of the framework. It has been layered to serve as the foundation for systematic, telemetry-based assessment and, as a consequence, systematic thinking about possibilities of proactive security monitoring mechanisms. It's possible to extend the framework into the domain of representative enterprise cloud telemetry and the extension research will be discussed and suitable MAE threshold strategies explored, for different workloads. There is also more integration available such as integration with cloud-native monitoring and automation tools for incidents. When it comes to applicability, it will be an opportunity to test and analyse in practice in terms of its size and feasibility in real world enterprise clouds that are dynamic in nature.

References

[1] Mohiyuddin, A., Javed, A. R., Chakraborty, C., Rizwan, M., Shabbir, M., & Nebhen, J. (2022). Secure cloud storage for medical IoT data using adaptive neuro-fuzzy inference system. International Journal of Fuzzy Systems, 24(2), 1203–1215. https://doi.org/10.1007/s40815-021-01104-y

[2] Ahmad, W., Rasool, A., Javed, A. R., Baker, T., & Jalil, Z. (2022). Cyber security in IoT-based cloud computing: A comprehensive survey. Electronics, 11(1), Article 16. https://doi.org/10.3390/electronics11010016

[3] Kiani, R., Keshavarzi, A., & Bohlouli, M. (2020). Detection of thin boundaries between different types of anomalies in outlier detection using enhanced neural networks. Applied Artificial Intelligence, 34(5), 345–377. https://doi.org/10.1080/08839514.2020.1722933

[4] Corallo, A., Lazoi, M., & Lezzi, M. (2020). Cybersecurity in the context of Industry 4.0: A structured classification of critical assets and business impacts. Computers in Industry, 114, Article 103165. https://doi.org/10.1016/j.compind.2019.103165

[5] Telikani, A., Gandomi, A. H., Choo, K. K. R., & Shen, J. (2022). A cost-sensitive deep learning-based approach for network traffic classification. IEEE Transactions on Network and Service Management, 19(1), 661–670. https://doi.org/10.1109/TNSM.2021.3112283

[6] ur Rehman, S., Khaliq, M., Imtiaz, S. I., Rasool, A., Shafiq, M., Javed, A. R., Jalil, Z., & Bashir, A. K. (2021). DIDDOS: An approach for detection and identification of distributed denial of service (DDoS) cyberattacks using gated recurrent units (GRU). Future Generation Computer Systems, 118, 453–466. https://doi.org/10.1016/j.future.2021.01.022

[7] Mittal, M., Iwendi, C., Khan, S., & Rehman Javed, A. (2021). Analysis of security and energy efficiency for shortest route discovery in low-energy adaptive clustering hierarchy protocol using Levenberg–Marquardt neural network and gated recurrent unit for intrusion detection system. Transactions on Emerging Telecommunications Technologies, 32(6), Article e3997. https://doi.org/10.1002/ett.3997

[8] Javed, A. R., Shahzad, F., ur Rehman, S., Zikria, Y. B., Razzak, I., Jalil, Z., & Xu, G. (2022). Future smart cities requirements, emerging technologies, applications, challenges, and future aspects. Cities, 129, Article 103794. https://doi.org/10.1016/j.cities.2022.103794

[9] Wang, R., & Ji, W. (2020). Computational intelligence for information security: A survey. IEEE Transactions on Emerging Topics in Computational Intelligence, 4(5), 616–629. https://doi.org/10.1109/TETCI.2019.2923426

[10] Tahaei, H., Afifi, F., Asemi, A., Zaki, F., & Anuar, N. B. (2020). The rise of traffic classification in IoT networks: A survey. Journal of Network and Computer Applications, 154, Article 102538. https://doi.org/10.1016/j.jnca.2020.102538

[11] Verma, A., & Ranga, V. (2020). Machine learning based intrusion detection systems for IoT applications. Wireless Personal Communications, 111(4), 2287–2310. https://doi.org/10.1007/s11277-019-06986-8

[12] Khan, F. A., Gumaei, A., Derhab, A., & Hussain, A. (2019). A novel two-stage deep learning model for efficient network intrusion detection. IEEE Access, 7, 30373–30385. https://doi.org/10.1109/ACCESS.2019.2899721

[13] Djenouri, Y., Belhadi, A., Lin, J. C. W., & Cano, A. (2019). Adapted k-nearest neighbors for detecting anomalies on spatio-temporal traffic flow. IEEE Access, 7, 10015–10027. https://doi.org/10.1109/ACCESS.2019.2891933

[14] Elsayed, M. S., Le-Khac, N. A., & Jurcut, A. D. (2020). INSDN: A novel SDN intrusion dataset. IEEE Access, 8, 165263–165284. https://doi.org/10.1109/ACCESS.2020.3022633

[15] Gill, S. S., Xu, M., Ottaviani, C., Patros, P., Bahsoon, R., Shaghaghi, A., Golec, M., Stankovski, V., Wu, H., Abraham, A., Singh, M., Mehta, H., Ghosh, S. K., Baker, T., Parlikad, A. K., Lutfiyya, H., Kanhere, S. S., Sakellariou, R., Dustdar, S., Rana, O., Brandic, I., & Uhlig, S. (2022). AI for next generation computing: Emerging trends and future directions. Internet of Things, 19, Article 100514. https://doi.org/10.1016/j.iot.2022.100514