



Digital Transformation
RESEARCH SOCIETY

Using AI for threat modeling in the context of 6G and IPS

Pos Doctoral: Prof. Dr. Wesley R. Bezerra
<wesley.bezerra@ifc.edu.br>

Supervisor : Prof. Dr. Carlos B. Westphall
<westphal@inf.ufsc.br>



UFSC - Laboratório
de Redes e Gerência

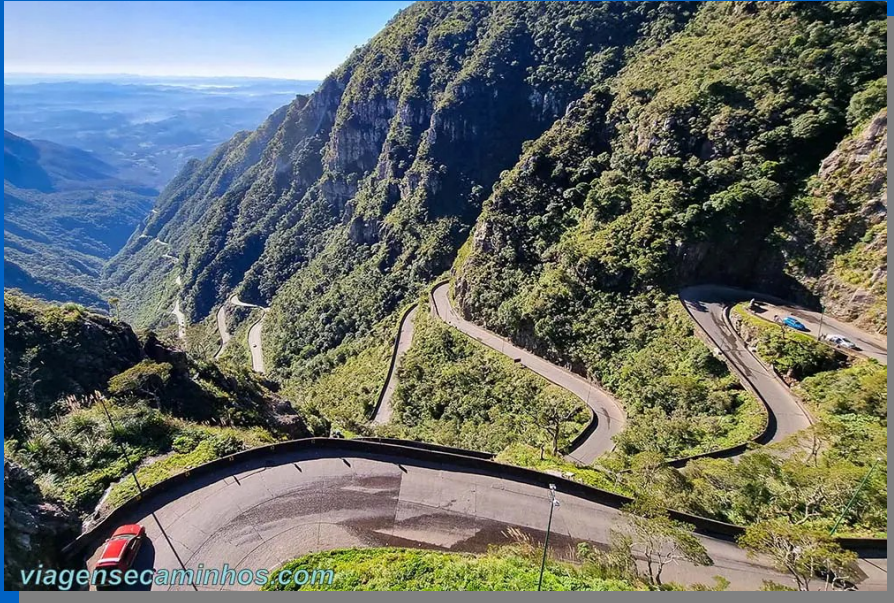
LRG

Resumé



Professor at the Federal Institute of Santa Catarina - Rio do Sul Campus. PhD in Computer Science from PPGCC/UFSC. Master's degree in Engineering and Knowledge Management from EGC/UFSC. Bachelor's degree in Information Systems from INE/UFSC. Bachelor's degree in Business Administration from Estácio de Sá.

Outline

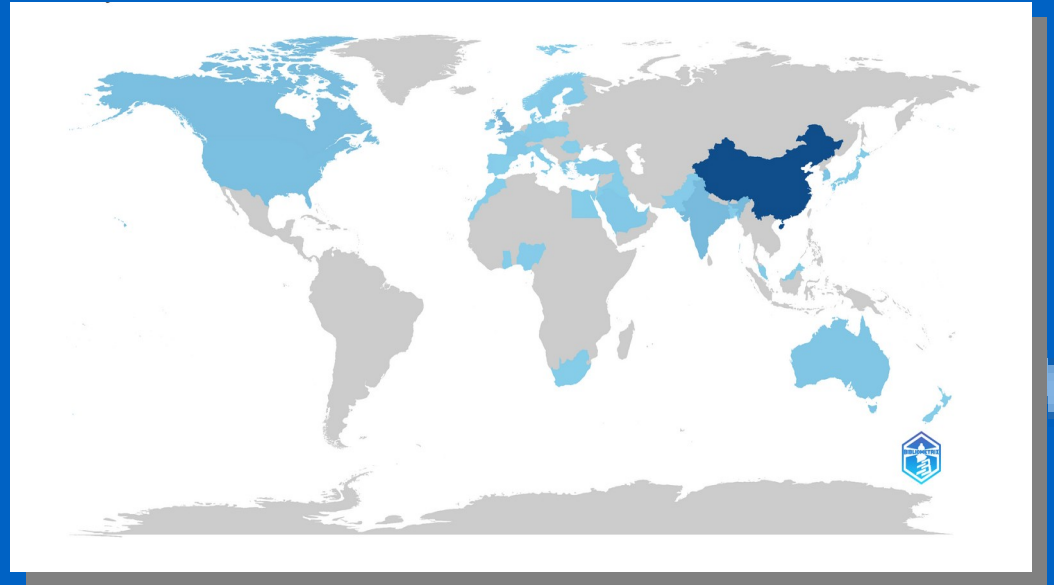


- Introduction
- Key Concepts
- What are we working on?
- Invitation



Introduction

- China's leading role
- Massive number of devices
- Integration/convergence between transmission modes
- Platform for higher quality digital services



Key Concepts

- 5G/6G
- Transmission Modes
- Threat Modeling
- Generative AI
- IPS – Intrusion Prevention System

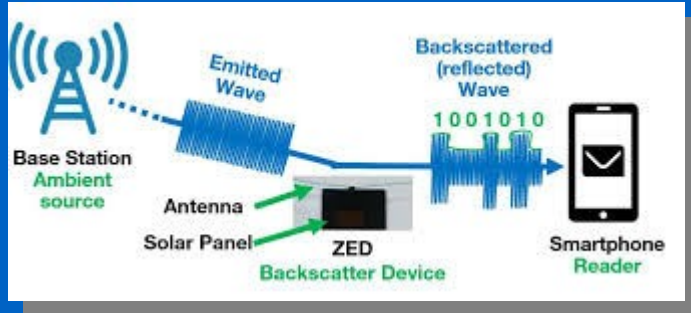


5G/6G

- MIMO and Massive MIMO
- Beamforming
- Terahertz
- AmbC
- RIS



[https://www.techmonitor.ai/leadership/
digital-transformation/what-is-massive-
mimo](https://www.techmonitor.ai/leadership/digital-transformation/what-is-massive-mimo)



<https://arxiv.org/pdf/2309.15040>

- **AmbC**

- Harms energy from radio waves
- It is not passive like RFID
- Processing and transmission
- It does not have a battery

Research paper

DDPG-AmBC: Dynamic reflection control for batteryless IoT networks with ambient backscatter

Edwardes A. Galhardo ^b ^a, Carlos B. Westphall ^a, Antonio Carlos de Oliveira Jr. ^b

Show more 

 Add to Mendeley  Share  Cite

<https://doi.org/10.1016/j.jnca.2026.104509> 

[Get rights and content](#) 

Under a Creative Commons license 

 Open access

Abstract

Batteryless Internet of Things (IoT) networks enabled by Ambient Backscatter Communication (AmBC) represent a promising approach for large-scale and energy-sustainable deployments. Yet, dense and time-varying environments introduce major challenges, such as unpredictable fluctuations in incident RF power, strong interference, and unstable link quality. These non-stationary

XLII BRAZILIAN SYMPOSIUM ON TELECOMMUNICATIONS AND SIGNAL PROCESSING - SBT 2025 SEPTEMBER 29TH TO OCTOBER 02ND, NATAL, RN

GAIA-DRL: A Geoenvironmental Agent for Energy Optimization in Batteryless IoT Networks with Ambient Backscatter

Edwardes A. Galhardo, Carlos B. Westphall, Wesley dos Reis Bezerra, and Antonio C. Oliveira Jr.

Abstract—This paper proposes GAIA-DRL, a framework that integrates ambient backscatter communication, geospatial intelligence, and deep reinforcement learning to optimize batteryless IoT networks. Real environmental data such as NDVI and pasture coverage are embedded into the agent's state vector, enabling adaptive, co-aware communication control. Using the DDPG algorithm, GAIA-DRL jointly optimizes throughput, latency, energy efficiency, and interference under dynamic conditions. Simulations with real geospatial layers demonstrate improvements in performance and sustainability. The approach supports low-cost, low-carbon applications in 6G-ready IoT systems, including greenhouse gas monitoring, smart agriculture, and sustainable environmental management.

Keywords—GAIA-DRL; Batteryless IoT; Ambient Backscatter; Geographic Information Systems (GIS); Remote Sensing; Deep Reinforcement Learning; Sustainable Networking.

I. INTRODUCTION

The acceleration of climate change and its cascading effects on ecosystems and agriculture demand innovative solutions for real-time environmental monitoring. Advances in low-power communication and artificial intelligence have enabled the development of smart, energy-efficient systems capable of capturing ecological dynamics with minimal infrastructure.

Wireless Sensor Networks (WSNs) have long supported environmental monitoring [1], but their dependence on batteries introduces logistical and ecological limitations for large-scale or remote deployments. Ambient Backscatter Communication (AmBC) emerges as a promising alternative, enabling battery-

less communication. Simultaneously, Geographic Information Systems (GIS) and remote sensing have become essential tools for tracking land-use changes, vegetation health, and environmental degradation. By combining in-situ IoT measurements with satellite-derived indices such as the Normalized Difference Vegetation Index (NDVI), researchers can build scalable and geospatially informed monitoring systems [6], [7].

In this work, we propose GAIA-DRL, a novel control algorithm for batteryless IoT networks. GAIA-DRL integrates spatial features such as NDVI and pasture coverage directly into the agent's state vector, enabling adaptive decision-making based on territorial and ecological priorities.

By combining AmBC, DRL, and geospatial intelligence, GAIA-DRL supports scalable, sustainable, and low-cost network architectures for applications in greenhouse gas tracking, precision agriculture, and smart environmental management.

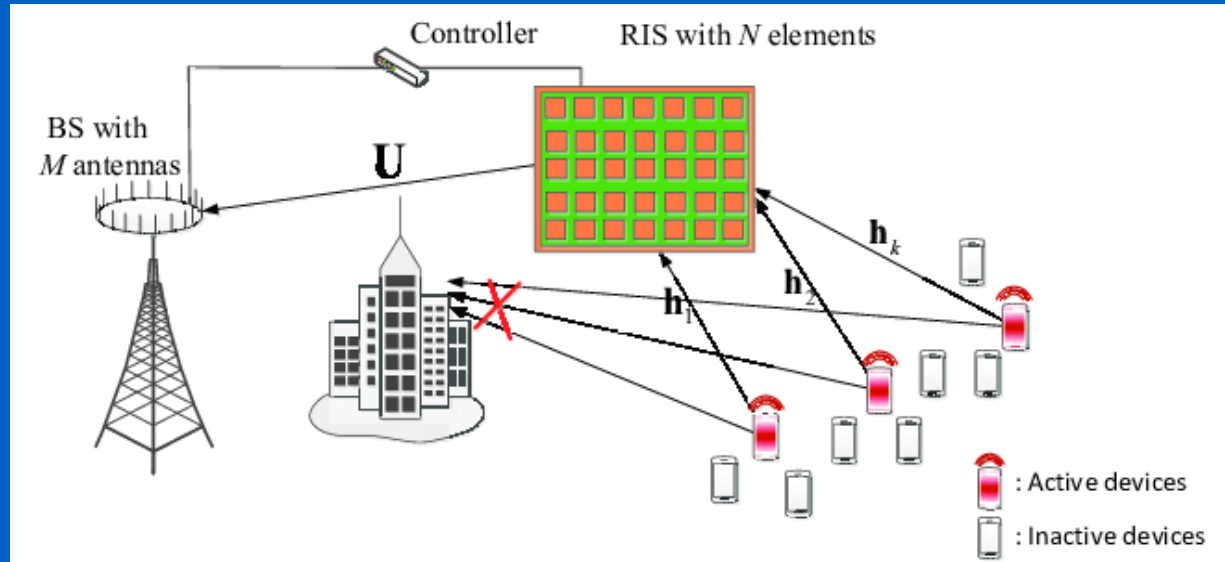
II. RELATED WORK

The design of intelligent and sustainable IoT networks has attracted growing research interest, particularly in applications involving remote sensing, energy efficiency, and environmental monitoring.

Batteryless IoT and Ambient Backscatter: Ambient backscatter communication (AmBC) has emerged as a key enabler of batteryless IoT, allowing ultra-low-power devices to transmit by reflecting existing RF signals [2]. Early implementations demonstrated passive communication with mini-

- **Reconfigurable Intelligent Surface (RIS)**

- Based on smart surfaces (new materials)
- Increased coverage
- Currently, there are already attacks focused on its data transmission layer.



https://www.researchgate.net/figure/RIS-aided-massive-unsourced-random-access-in-6G-wireless-networks-with-blocked-direct_fig1_354141168



Transmission Modes



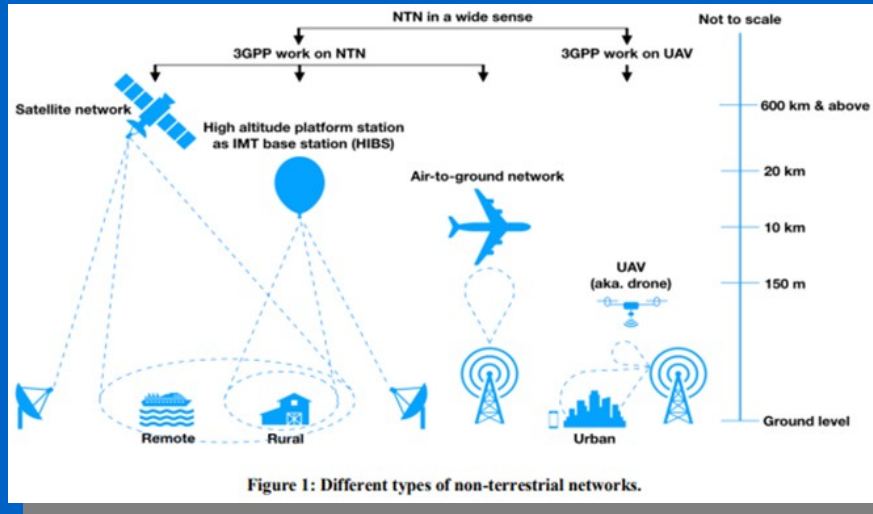
- **Via satellite**
 - Geostationary (GEO)
 - Medium Earth Orbit (MEO)
 - Low Earth Orbit (LEO)



<https://www.eetasia.com/vicor-power-modules-boost-satellite-internet-constellations/>

- **Non-Terrestrial Network (NTN)**

- Satellites
- Balloons
- Airplanes
- UAVs

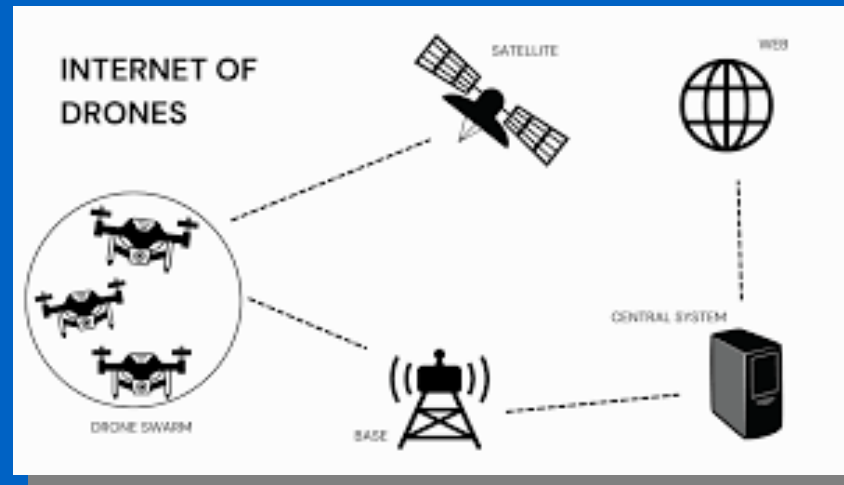


<https://www.5gamericas.org/non-terrestrial-networks-could-be-the-next-frontier-for-5g/>

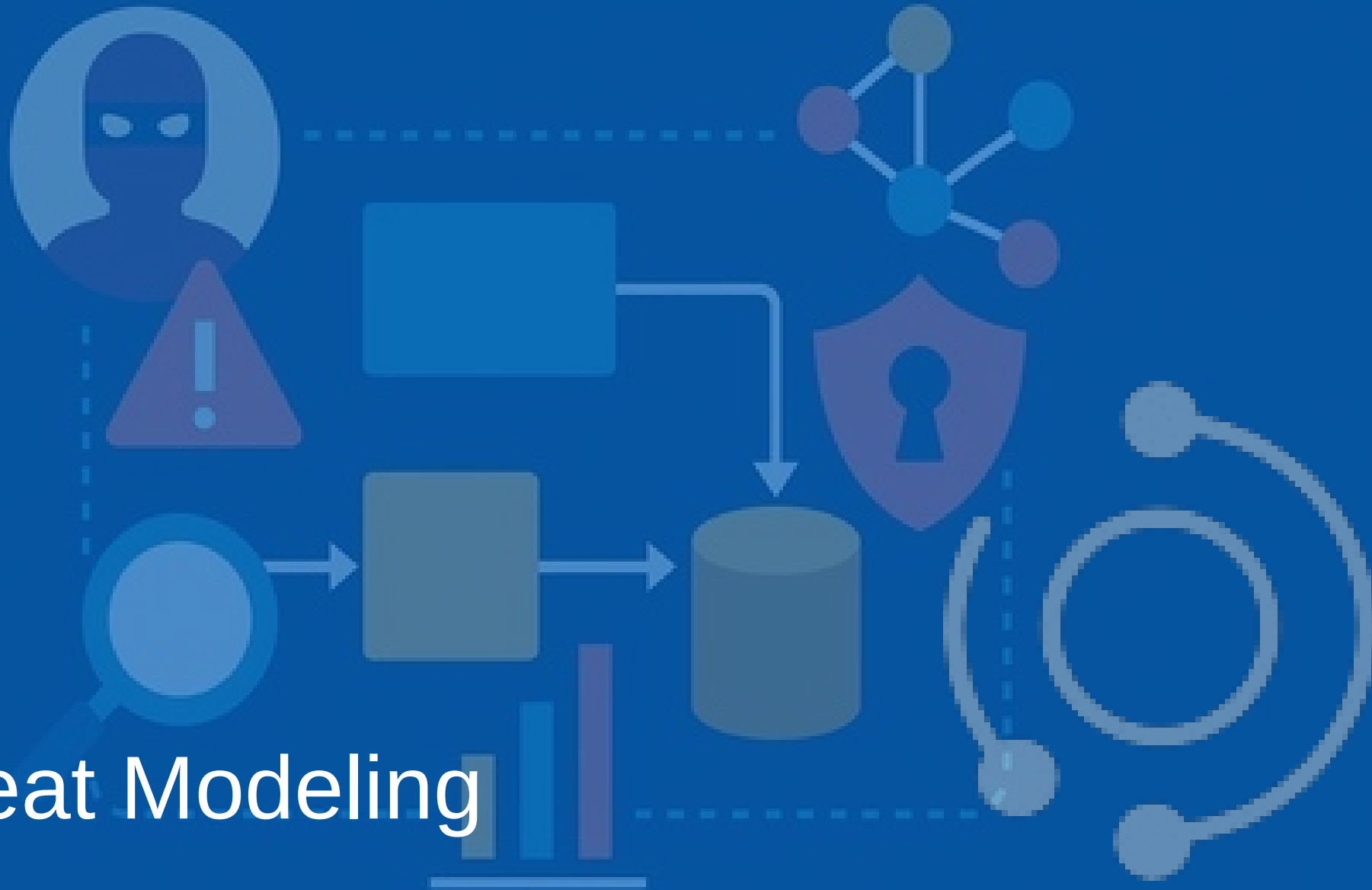


- **UAV**

- Integration with other modes of transport
- Mobility
- Remote/rural environments



Threat Modeling

A conceptual diagram for threat modeling on a blue background. It features a central flow from a magnifying glass to a square block to a cylinder. A laptop icon is above the flow, and a shield with a keyhole is to the right. A hacker icon with a warning triangle is on the left, and a network graph is at the top right. A bar chart is at the bottom center, and a circular flow diagram is on the right. Dashed lines connect the hacker icon to the top and bottom network graphs.

- A modeling workflow for complex systems has been developed and can be automated.
- Tests have been completed but not yet published.



Journal of Open Innovation: Technology, Market,
and Complexity

Volume 11, Issue 4, December 2025, 100654



HyVAW: A hybrid vulnerability analysis workflow threat model methodology for complex systems based on distributed components ☆

Wesley dos Reis Bezerra¹  , Cristiano Antonio de Souza¹ , Carla Merkle Westphall¹ , Carlos Becker Westphall¹ 

[Show more](#) ▼

[+](#) Add to Mendeley [Share](#) [Cite](#)

<https://doi.org/10.1016/j.joitmc.2025.100654> [Get rights and content](#) ▶

Under a Creative Commons [license](#) ▶ ● [Open access](#)

Characteristics and Main Threats about Multi-Factor Authentication: A Survey

WR Bezerra^{a,c,*,1} (Phd Candidate), CA de Souza^{a,c,*,1} (Phd Candidate), CM Westphall^{a,c,*,1} (Phd) and Carlos B. Westphall^{a,*} (Advisor)

^aUFSC - Federal University of Santa Catarina, Campus Universitário - Trindade, Florianópolis/SC - Brazil, 88040-380

ARTICLE INFO

Keywords:

threat model
multi-factor authentication
security
smart citie

ABSTRACT

This work reports that the Systematic Literature Review process is responsible for providing theoretical support to research in the Threat Model and Multi-Factor Authentication. However, different from the related works, this study aims to evaluate the main characteristics of authentication solutions and their threat model. Also, it intends to list characteristics, threats, and related content to a state-of-art. As a result, we brought a portfolio analysis through charts, figures, and tables presented in the discussion section.

1. Introduction

This work reports that the Systematic Literature Review process is responsible for providing theoretical support to research in Threat Model (TM) and Multi-Factor Authentication (MFA). Also, it aims to build a bibliographic portfolio capable of guiding the discussions and being theoretical support necessary for putting forward the previously cited research areas.

<https://arxiv.org/pdf/2209.12984>

Security Aspects in an Intelligent Lighting System for Public Squares using Fog Computing

Wesley R. Bezerra¹, Cristiano A. Souza¹, Carla M. Westphall¹, Carlos B. Westphall¹

¹LRG – Universidade Federal de Santa Catarina (UFSC)
Florianópolis – SC – Brazil

{wesleybez, cristianoantonio.souza10, carlosbwestphall1}@gmail.com,
carla.merkle.westphall@ufsc.br

Abstract. Security in public spaces is a fundamental factor for citizens and can be provided by digital tools such as remote sensing. However, the security of such tools is also an important issue, and violating this security can lead to the susceptibility of loss of security in public spaces. This work presents a use case where an authentication solution is applied to ensure security in a smart lighting system in public squares. The use case, the adversary and its motivation, the threat modeling of the system, and a general discussion about this study are presented. As a result, a threat model with countermeasures is presented, and security aspects brought about by the use of the adopted multi-factor authentication mechanism with reputation are discussed.

1. Introduction

Security in Internet of Things (IoT) devices has been a concern and research subject over the last few years [Deep et al. 2019]. According to some authors [Yi et al. 2015, ?, ?], the

<https://sol.sbc.org.br/index.php/courb/article/download/35261/35051>

A Bibliometrics Analysis on 28 years of Authentication and Threat Model Area

WR Bezerra^{a,c,**,1} (Phd Candidate), CA de Souza^{a,c,**,1} (Phd Candidate), CM Westphall^{a,c,**,1} (Phd) and Carlos B. Westphall^{a,*} (Advisor)

^aUFSC - Federal University of Santa Catarina, Campus Universitário - Trindade, Florianópolis/SC - Brazil, 88040-380

ARTICLE INFO

Keywords:
threat model
authentication
security
bibliometrics

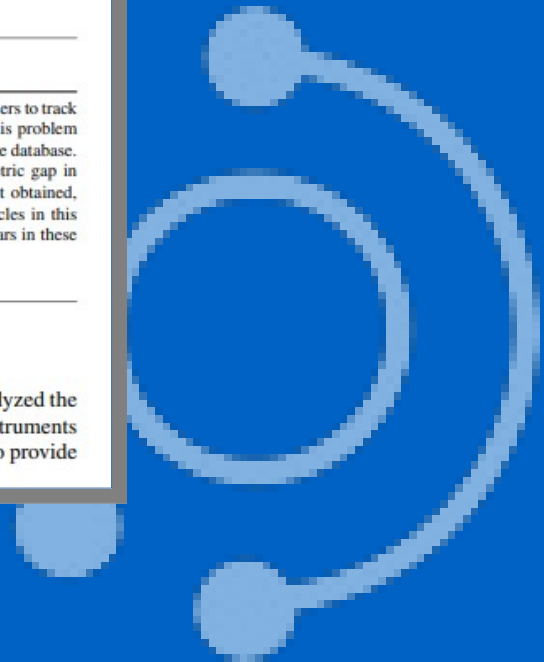
ABSTRACT

The large volume of publications in any research area can make it difficult for researchers to track their research areas' trends, challenges, and characteristics. Bibliometrics solves this problem by bringing statistical tools to help the analysis of selected publications from an online database. Although there are different works in security, our study aims to fill the bibliometric gap in the authentication and threat model area. As a result, a description of the dataset obtained, an overview of some selected variables, and an analysis of the ten most cited articles in this selected dataset is presented, which brings together publications from the last 28 years in these areas combined.

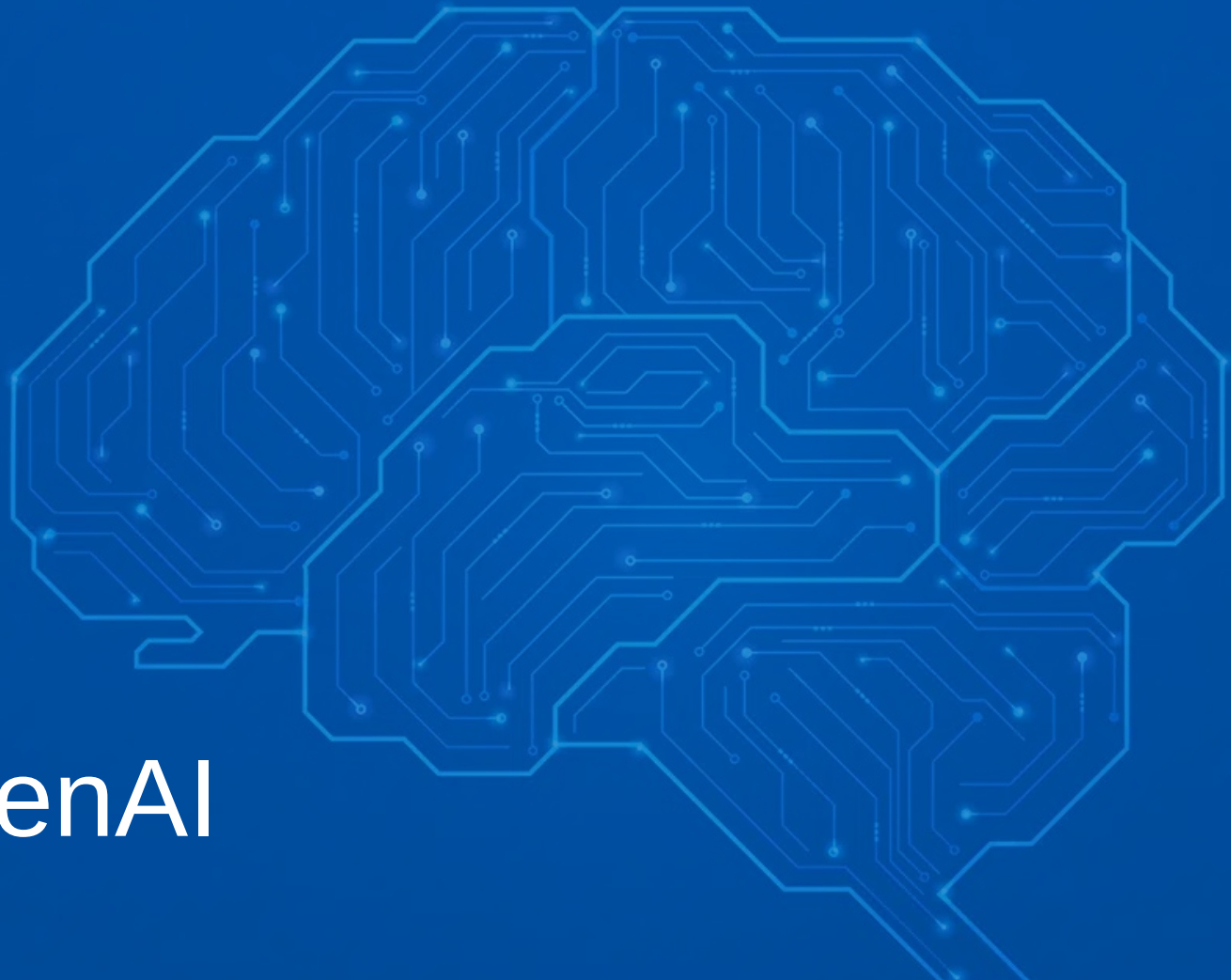
1. Introduction

Robust analysis is based on data and instruments applied to obtain these data. Regarding it, this study analyzed the results of the database gathered in scientific publications portals using bibliometrics instruments. Such instruments were part of the threat model proposal for a Ph.D. thesis; however, it is not limited to this purpose and can also provide a bibliometric basis for any studies involving authentication and threat model.

<https://arxiv.org/pdf/2209.12985>



GenAI



- Research on authentication and GenAI was conducted in the previous stage.
- It supported the current stage proposal and identified this research opportunity.



- Problems:
 - Identification
 - Fake news
 - Deep fake (audio and video)
 - Legislation
 - Phone Calls
 - Accountability



[Home](#) / [Proceedings](#) / [ICOIN](#) / [ICOIN 2026](#)

2026 40th International Conference on Information Networking (ICOIN)

Identifying Fakes in Social Media Text Messages Using Stylometry

Year: 2026, Pages: 581-586

DOI Bookmark: [10.1109/ICOIN68469.2026.11480532](https://doi.org/10.1109/ICOIN68469.2026.11480532)

Authors

[Cristian G. Butzke](#), BCC/ IFC, Rio do Sul, Brazil

[Marcelo L. Brocardo](#), ESAG/ UDESC, Florianópolis, Brazil

[Wesley R. Bezerra](#), BCC/ IFC, Rio do Sul, Brazil

[Carlos B. Westphall](#), PPGCCI UFSC, Florianópolis, Brazil



DOWNLOAD PDF



SHARE ARTICLE

GENERATE CITATION

Abstract

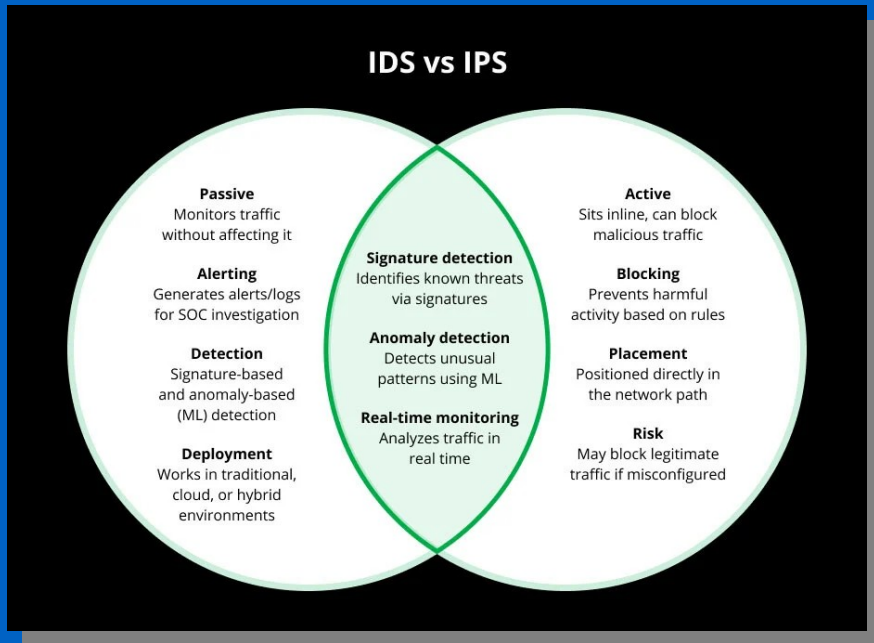
The authentication and authenticity of artifacts have been subverted for unsavory purposes, such as creating fake texts and other artifacts and trying to impersonate a user. Authentication has also been affected by the impersonation of some aspects of biometrics, potentially compromising the identification of subjects. In this perspective, this work proposes a continuous authentication solution that uses textual features to identify stylometric aspects using a Support Vector Machine to identify the authenticity and authorship of texts from the X/Twitter social network. As a result, the results obtained through different kernel configurations for different users are presented. Additionally, a simulator of social media publications infers the authenticity and authorship of the published text based on previously trained machine learning.



Intrusion Prevention System

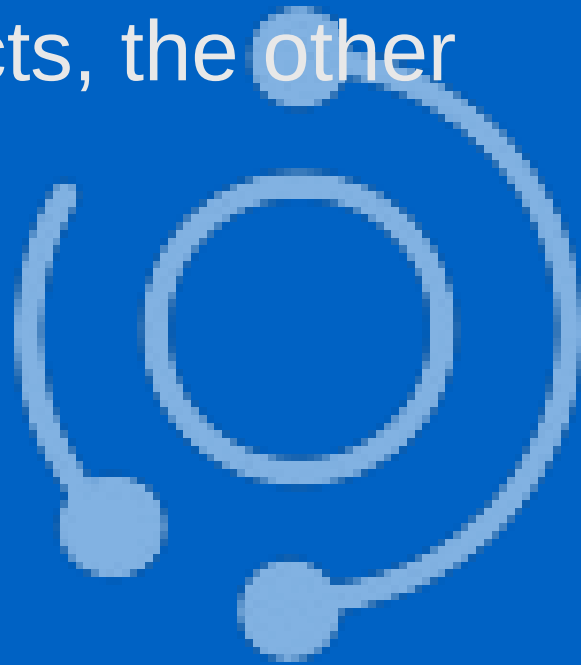


IDS e IPS

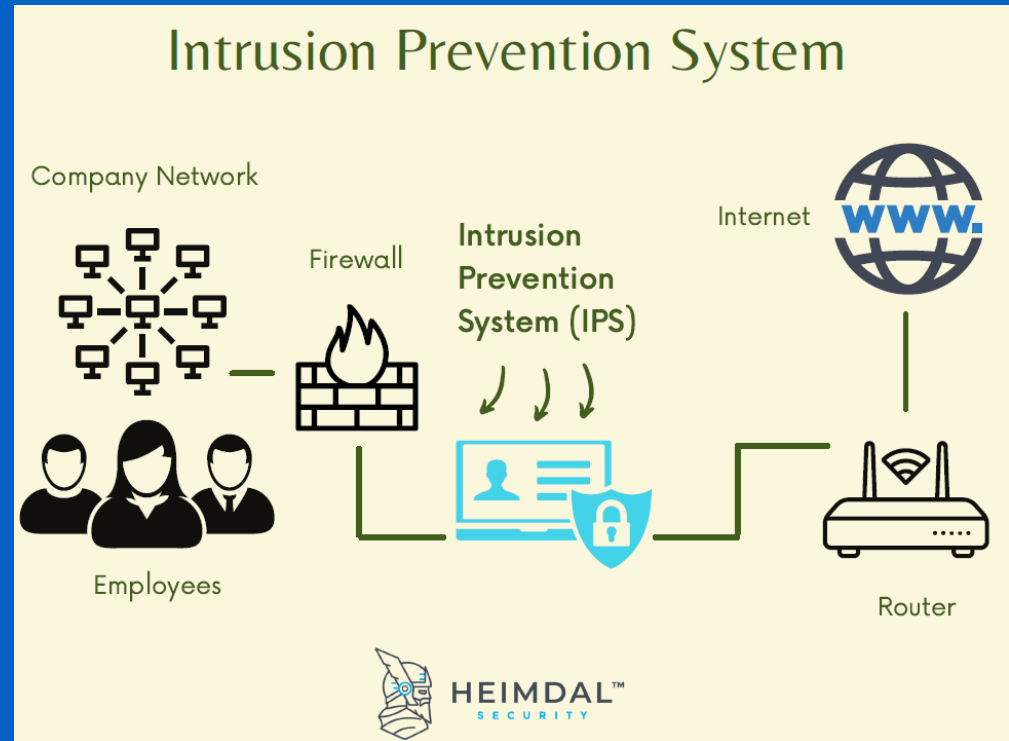


<https://corelight.com/resources/glossary/ids-vs-ips>

- Both are anti-intrusion systems.
- One detects, the other prevents.



- An IPS (Intrusion Prevention System) is a more proactive approach to the problem of attempted intrusions.



Their main difference, and where an inherent complexity lies in the process, is that the IDS identifies the occurrence of a breach, while the IPS works to prevent it; that is, it works with active monitoring and iteration on the network to prevent the attempt from materializing.



Some IDS and IPS approaches have adopted explainable AI (XAI), machine learning, P2DR (protection, policy, detection, and response) models, and deep learning; which shows the need for a more dynamic approach, ready for the upcoming challenges of 6G.



DNNET-Ensemble approach to detecting and identifying attacks in IoT environments

Cristiano A. de Souza¹, Carlos B. Westphall¹, Jean D. G. Valencio²
Renato B. Machado², Wesley dos R. Bezerra¹

¹Departamento de Informática – Universidade Federal de Santa Catarina (UFSC)

²Universidade Estadual do Oeste do Paraná (UNIOESTE)

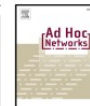
cristiano.souza.c@posgrad.ufsc.br, westphal@inf.ufsc.br

renato.machado@unioeste.br, jean.valencio@unioeste.br

wesley.bezerra@ifc.edu.br

Abstract. Special security techniques like intrusion detection mechanisms are indispensable in modern computer systems. It is important to detect and identify the attack in a category so that specific countermeasures for the threat category are solved. However, most existing multiclass detection approaches have some weaknesses, mainly related to detecting specific categories of attacks and problems with false positives. This article addresses this research problem and advances state-of-the-art, bringing contributions to a two-stage detection architecture called DNNET-Ensemble, combining binary and multiclass detection. The results obtained in experiments with renowned intrusion datasets demonstrate that the approach can achieve superior detection rates and false positives performance compared to other state-of-the-art approaches.

<https://sol.sbc.org.br/index.php/sbr/article/download/24556/24377>



Survey paper

Hierarchical multistep approach for intrusion detection and identification in IoT and Fog computing-based environments[☆]

Cristiano Antonio de Souza^{a,*}, Carlos Becker Westphall^a, Jean Douglas Gomes Valencio^b,
Renato Bobsin Machado^b, Wesley dos R. Bezerra^a

^a Federal University of Santa Catarina, Florianópolis, SC, Brazil

^b State University of Western Paraná, Foz de Iguaçu, PR, Brazil



ARTICLE INFO

Keywords:

Internet of Things
Fog computing
Intrusion detection and identification
Deep neural networks
Ensemble learning

ABSTRACT

Special security techniques, such as intrusion detection mechanisms, are indispensable in modern computer systems. With the emergence of the Internet of Things they have become even more important. It is important to detect and identify the attack in a category so that countermeasures specific to the threat category can be resolved. However, most existing multiclass detection approaches have some weaknesses, mainly related to detecting specific categories of attacks and problems with false positives. This article addresses this research problem and advances state-of-the-art, bringing contributions to a two-stage detection architecture called DNNET-Ensemble, combining binary and multiclass detection. While the benign traffic can be quickly released on the first detection, the intrusive traffic can be subjected to a robust analysis approach without causing delay issues. Additionally, we propose the DNNET binary approach for the binary detection level, which can provide more accurate and faster binary detection. We present the proposal of a federated strategy to train the neural model of the DNNET method without sending data to the cloud, thus preserving the privacy of local data. The proposed Hybrid Attribute Selection strategy can find an optimal subset of attributes through a wrapper method with a lower training cost due to pre-selection using a filter method. Furthermore, the proposed Soft-SMOTE improvement allows operating with a balanced dataset with a minor training time increase, even in scenarios where there are a large number of classes with a large imbalance among them. Results obtained from experiments on renowned intrusion datasets and laboratory experiments demonstrate that the approach can achieve superior detection rates and false positive performance compared to other state-of-the-art approaches.

<https://www.sciencedirect.com/science/article/pii/S1570870524001525>

Next jobs in line

- Literature Mapping of 6G Transmission Modes
- Literature Mapping of Datasets for 6G
- Scope Review on TM and 6G



CONFERENCE PROCEEDINGS

[<](#)
Previous[Next](#) >[☰ Table of Contents](#)[📄 Similar Articles](#)

[Home](#) / [Proceedings](#) / [ICOIN](#) / [ICOIN 2026](#)

2026 40th International Conference on Information Networking (ICOIN)

Intrusion Detection of Data Manipulation Attack in IoT Network Based on Fog Computing

Year: 2026, Pages: 894-899

DOI Bookmark: [10.1109/ICOIN68469.2026.11480483](#)

Authors

[Justino Augusto Da Silva](#), Federal University of Santa Catarina, Department of Informatics and Statistics, Florianópolis, Brazil

[Carlos Becker Westphall](#), Federal University of Santa Catarina, Department of Informatics and Statistics, Florianópolis, Brazil

[Wesley Dos Reis Bezerra](#), Federal University of Santa Catarina, Department of Informatics and Statistics, Florianópolis, Brazil

[📄 DOWNLOAD PDF](#)[▼ SHARE ARTICLE](#)[GENERATE CITATION](#)

Abstract

Security in Internet of Things (IoT) environments supported by Fog Computing is challenged by data manipulation attacks, which can compromise critical systems. This work presents a twofold contribution: (i) a systematic mapping of the literature on intrusion detection techniques in IoT-Fog and (ii) an experimental evaluation using the ToN-IoT dataset. Four supervised algorithms (RF, KNN, XGBoost, and SVM) were compared. The results show that RF and XGBoost achieved metrics above 0.99 in precision, recall, F1-Score, and AUC, while SVM presented high recall (0.988) but low precision (0.83). This study reinforces that ensemble learning-based models are promising for mitigating attacks in IoT-Fog.

Threats + AI + 6G

CONFERENCE PROCEEDINGS



◀

Previous

Next

▶

☰

Table of Contents

📄

Similar Articles

Home / Proceedings / ICOIN / ICOIN 2026

2026 40th International Conference on Information Networking (ICOIN)

Threats and Ai Trends in Threat Modeling for 5G/6G

Year: 2026, Pages: 645-649

DOI Bookmark: 10.1109/ICOIN68469.2026.11480655

Authors

Wesley R. Bezerra, BCC/ IFC Rio do Sul-SC,Brazil

Edwardes A. Galhardo, UFG GO,Brazil

Lais M. Bezerra, SENAI SC,Brazil

Carlos B. Westphall, PPGCC/ UFSC Florianópolis,Brazil

📄

DOWNLOAD PDF

▼

SHARE ARTICLE

GENERATE CITATION

Abstract

With the increase in the attack surface provided by the advancement of **5G/6G**, concerns about attacks and security breaches also increase. Since this is a recent area of research and development, some challenges are encountered. Furthermore, with the increase in capillarity and the number of connected devices promoted by technologies such as Reconfigurable Intelligent Surface, attacks that can exploit connected devices may become a problem since these devices will have a considerable number. With the perspective of providing a future vision for the solutions that were in threat modeling and a current view of the threats researched in this topic, we bring an analysis of articles that address threat analysis in 5G/6G and Reconfigurable Intelligent Surface, presenting their results and considerations through a qualitative analysis of the challenges encountered.



Machine learning + authentication

CONFERENCE PROCEEDINGS



Home / Proceedings / ICOIN / ICOIN 2026

2026 40th International Conference on Information Networking (ICOIN)

Identifying Fakes in Social Media Text Messages Using Stylometry

Year: 2026, Pages: 581-586
DOI Bookmark: 10.1109/ICOIN68469.2026.11480532

Authors

Cristian G. Butzke, BCC/ IFC, Rio do Sul, Brazil
Marcelo L. Brocardo, ESAG/ UDESC, Florianópolis, Brazil
Wesley R. Bezerra, BCC/ IFC, Rio do Sul, Brazil
Carlos B. Westphall, PPGCCI UFSC, Florianópolis, Brazil

[Download PDF](#)[Share Article](#)[Generate Citation](#)

[Previous](#)[Next](#)

[Table of Contents](#)[Similar Articles](#)

Abstract

The authentication and authenticity of artifacts have been subverted for unsavory purposes, such as creating fake texts and other artifacts and trying to impersonate a user. Authentication has also been affected by the impersonation of some aspects of biometrics, potentially compromising the identification of subjects. In this perspective, this work proposes a continuous authentication solution that uses textual features to identify stylometric aspects using a Support Vector Machine to identify the authenticity and authorship of texts from the X/Twitter social network. As a result, the results obtained through different kernel configurations for different users are presented. Additionally, a simulator of social media publications infers the authenticity and authorship of the published text based on previously trained machine learning.

IDS + Fog Computing + DataSets

CONFERENCE PROCEEDINGS



← Previous

Next →

 Table of Contents

 Similar Articles

[Home](#) / [Proceedings](#) / [ICOIN](#) / [ICOIN 2026](#)

2026 40th International Conference on Information Networking (ICOIN)

Intrusion Detection of Data Manipulation Attack in IoT Network Based on Fog Computing

Year: 2026, Pages: 894-899
DOI Bookmark: [10.1109/ICOIN68469.2026.11480483](https://doi.org/10.1109/ICOIN68469.2026.11480483)

Authors

Justino Augusto Da Silva, Federal University of Santa Catarina, Department of Informatics and Statistics, Florianópolis, Brazil
Carlos Becker Westphall, Federal University of Santa Catarina, Department of Informatics and Statistics, Florianópolis, Brazil
[Wesley Dos Reis Bezerra](#), Federal University of Santa Catarina, Department of Informatics and Statistics, Florianópolis, Brazil

 [DOWNLOAD PDF](#)

 [SHARE ARTICLE](#)

[GENERATE CITATION](#)

Abstract

Security in Internet of Things (IoT) environments supported by Fog Computing is challenged by data manipulation attacks, which can compromise critical systems. This work presents a twofold contribution: (i) a systematic mapping of the literature on intrusion detection techniques in IoT-Fog and (ii) an experimental evaluation using the ToN-IoT dataset. Four supervised algorithms (RF, KNN, XGBoost, and SVM) were compared. The results show that RF and XGBoost achieved metrics above 0.99 in precision, recall, F1-Score, and AUC, while SVM presented high recall (0.988) but low precision (0.83). This study reinforces that ensemble learning-based models are promising for mitigating attacks in IoT-Fog.

auth + genai

Authentication Challenges in Generative AI Era: a mapping review

1st Wesley dos Reis Bezerra
PPGCC/CTC

Federal University of Santa Catarina
Florianópolis, Brazil
wesleybez@gmail.com
0000-0002-6098-7172

2nd Laís Machado Bezerra
SENAISC

SC, Brazil
lais.machado1@gmail.com
0000-0003-3331-7277

3rd Given Name Surname
PPGCC/CTC

Federal University of Santa Catarina
Florianópolis, Brazil
carlosbwestphall@gmail.com
0000-0002-5391-7942

Abstract—Authentication and authenticity have been a security challenge since the beginning of information sharing, especially in the context of digital information. With the advancement of generative artificial intelligence, these challenges have evolved, demanding a more up-to-date analysis of their impacts on society and system security. This work presents a mapping review that analyzed 88 documents from the IEEE Explorer, Scopus, and ACM databases, promoting an analysis of the resulting portfolio through six guiding questions focusing on the most relevant work, challenges, attack surfaces, threats, proposed solutions, and gaps. Finally, the portfolio articles are analyzed through this guiding research lens and also receive individualized analysis. The results consistently outline the challenges, gaps, and threats related to images, text, audio, and video, thereby supporting new research in the areas of authentication and generative artificial intelligence.

Index Terms—component, formatting, style, styling, insert

prejudices) or even the lack of knowledge among other media users, such as video users, who are deceived by deepfakes.

The rest of the work is organized as follows: Section II presents an overview of the methodology used for the systematic literature review. Following, Section III provides a brief discussion of the challenges encountered through the systematic review. Concluding with the Section IV, which presents the conclusions and vision for the future development of new work in the area.

II. METHODOLOGY

A. Objectives and Research Question

This work focused on security aspects of GenAI, providing a broader view of the challenges and how they materialize in the real world. Some authentication and authenticity challenges

this conference



Invitation

- Anyone interested in publishing partnerships or collaborations, even small ones, can contact me by email.
- I enjoy doing literature reviews and reading a lot.



References

- <https://arxiv.org/pdf/2309.15040>
- https://www.researchgate.net/figure/An-illustration-of-RIS-assisted-secure-AmBC-networks_fig1_378201676
- <https://www.cervoz.com/company/news/leo-satellite-in-5g-networks/detail>
- <https://semiengineering.com/low-earth-orbit-satellites-for-more-reliable-internet/>
- <https://corelight.com/resources/glossary/ids-vs-ips>



Questions and Suggestions

E-mail:

- **wesley.bezerra@ifc.edu.br**

- Google Scholar:

**[https://scholar.google.com/citations?
user=14mGOg0AAAAJ&hl=en-US](https://scholar.google.com/citations?user=14mGOg0AAAAJ&hl=en-US)**

