

ISSN 2047-3338

Analyzing Internet Traffic Dynamics for Enhanced Emergency Response in IoT Environments

Nimra Latif, Muhammad Umar Sultan

Department of Computer Science and Engineering, University of Engineering and Technology, Lahore

Abstract– In this research, we address the flow of internet traffic patterns and the safety of message exchange in this work, with M2M (machine-to-machine) communication technology. By analyzing the whole dataset from different IoT machines and also mimicked attacks, we wish to uncover traffic flows, detect abnormality and prescribe security approaches to improve the emergency communication networks defense. Data are subjected to advanced analysis methods by us in order show the weak areas as well as ethical considerations. Our objective is also to help to avoid the risks to data privacy and security. We believe our discoveries to be a basic step toward coping strategies improvements that put in place reliable emergency and situation communication infrastructure.

Index Terms– Internet Traffic, Emergency Response, IoT Environment and Strategies

I. INTRODUCTION

THE presence of connecting devices and systems in the digital era, which is marked by an unprecedented pace of technological evolution and innovation, is applied to M2M communication as a groundbreaking approach of connectivity and innovation. An interactive discovery of the M2M communication universe is the main goal of this introductory part that will thoroughly review internet traffic regulation and active services security standards.

M2M communication still carries out the revolution in the way devices communicate and interact, insisting on the removal of the middleman particularly human [1]. This transformative technology has therefore revolutionized connectivity and allowed to build a global networking which is able to comprise devices working across different laboratories, such as industrial automation, smart cities, and even healthcare systems. Given that modern society is incredibly dependent on the IoT, getting the grasp of M2M networks is vital, especially for urgent tasks including emergency services.

The combined creation of M2M communications with public emergency services proves a vital and essential point in blocking where each situation meets the urgent calls for aid. In emergency situations, fast and accurate message exchange is not only important but vital to ensure the safe condition of the population and, therefore, reduce the potential risks [11]. Yet, the movement of data flow during and after the shrinking of emergency services renders the complexity of matters

cyclically, adding an extra burden which must be thoroughly scrutinized and investigated. All data packets contain information that could have an impact on timeliness of response the decisions. Hence, it is necessary to discover patterns as well as detect vulnerabilities that are present in the network in the probing process.

However, as we begin the task of finding out the intersection of M2M communication with emergency system, it becomes more convinced of the fact that it provides opportunities as well as challenges. However, whereas the bewitching flow of data would be able to improve the emergency response systems effectiveness, its infrastructure would become vulnerable to possible faults and hazards. Through the process of untangling the complexities of signal trafficking and safety precautions, we will discover the different perspectives that will lead us in the way of creating resilient schemes that are specialized for the M2M communication during the active intervention services.

II. BACKGROUND AND MOTIVATION

The spread of the internet on which any communication and identifiers are based as well as the set of internet infrastructure and connection devices has resulted in connectivity having an influence on each aspect of human endeavors. These smart phones, and other types from smart watches, industrial sensors and even autonomous vehicles, are a network of interconnected devices that build the main infrastructure of today's communication framework. At the core of this interwoven fiber system managing the interactions is a Machine-to-Machine communication (M2M) domain, where devices are functioning stress-free without any involvement of humans [12].

In the field of emergency services where every second is crucial to communication as any delay may be the only thing that can separate between living and death the value of M2M communications increases tremendously. Emergency services people use data transmission and communication which are based on live time to be able to do strategic acquisition of information, reduce dangers, and rapid intervention, respectively. Nevertheless, the delicate thread of internet traffic pattern collapse during active emergency

carries mixed baggage, meaning new approaches emerged together with new problems to be addressed.

III. RESEARCH OBJECTIVES

Summarizing it all, this research seeks to examine the minor details of information traffic in an emergency when the M2M communication is underway, then prepare strategies of unreachable security measures for this critical case. To achieve this objective, the following specific goals are delineated: To achieve this objective, the following specific goals are delineated:

i). Analysis of Internet Traffic Patterns: Carry out a multilayered internet traffic patterns analysis for instances of ongoing emergency services and usage of our own data set containing the 'normal' as well as 'adversarial' network behaviors.

ii). Identification of Security Threats: Find out all the possible security threats and loopholes in M2M communication during high-pressure situations for instance DDoS attacks, brute-force SSH attacks, and similar IP address scanning techniques.

iii). Development of Security Measures: Formulate and implement precise security methodologies and procedures to reduce the perceived risks and become more robust in emergency communication scenarios during active emergency response services.

iv). Ethical Considerations: Reinforce ethical aspects in data privacy and security, which has must utilized in a manner that guarantees a responsible and secure communication channel while successfully attacking the need of information exchange with a certain degree of individual privacy entitlements.

IV. RELATED WORK

Transformer Architectures in M2M Communication: [1] This article will focus on a very thorough investigation of transformer architectures used by natural language processing in the context of M2M connection. It illustrates how machine learning moves from a traditional approach to the model based on transformer to show how these models can fully analyze and discover long-range trends in network traffic. An original literature review is conducted to assess the development of the transformer network architectures customized for the machine-to-machine communication batches. Data clearly demonstrated that there are pros and cons with integrating transformers for M2M communications ecosystems.

Convolutional Neural Networks (CNNs) for Internet Traffic Analysis: The contribution that CNNs bring in analyzing internet traffic patterns will therefore serve as the study's key reference. [2] The study, therefore, will focus on the application and development of CNNs. There are such details as CNN progresses in relation to the network information and so emphasizes the fact that CNN is primary in identifying the spatial patterns. Like an in-depth literature analysis based on various CNN architectures and their efficiency rates at internet traffic analysis tasks will be outlined. This research is not only meant to help us see how CNN is used as a base model of M2M communications, but also to propose new learning algorithms that improve M2M systems.

Visualization Techniques in Network Traffic Analysis: Besides decoding the network data, it is also imperative that we create visualizations of the network that can be used to demonstrate the insight that we have drawn from various analyses. [3] This paper deals with the various visualization methods that form the mainstay of network traffic analysis, which not only provide a means to display complex network signals in a visually understandable form. Such a review concerns the diversity of available visualization methods, including standard procedures, as well as methods, employing state-of-the-art deep learning approaches. It is from this point of positing the landscape of network data visualization that the paper drives toward cutting-edge methods for devising the e-textured and comprehensible model in M2M communication environment.

Temporal Dynamics in Internet Traffic: The investigation of how internet traffic is changing over time is a salient element of proficient communication commissions. [5] This paper focuses on the modeling of temporal aspects of network signals, with special attention given to the mathematical approaches used in capturing the changing dynamics over time. Involvement of experimentation on network datasets with complicated temporality will be the key factor in the study to comply with the possible hurdles posed by dynamic network activity. Building up such knowledge is not only crucial in pushing for adaptive communications systems that would suit the crisis situations in M2M networks but would also open up the channel for other manufacturers in ensuring that there is a joint framework that underlines networks resiliency during disaster situations.

Real-time Communication Protocols for Emergency Services: While more and more real-time communication is required in crisis management, the course of this article is to review the existing protocols and systems. [6] This paper argues that tight communication delay is essential in emergency circumstances and considers what the best real-time communications protocols from among those available can offer. To the reasons of which the study underlined the relevance of the M2M communication in the case of emergency services is very likely the contribution would be a higher response rate and consistent communication among the emergency responders.

Ethical Considerations in M2M Communication for Emergency Services: Next to technological breakthroughs, however, ethical considerations turn out to be the watershed in embedded machine communication for the field of emergency services. [7] This paper is focused on evaluating ethics issues as data security, privacy, and consent in the M2M networks of communication during primary emergencies. The paper will be focused on reviewing all the ethical directives and conditions existing currently. The objective will be to lead to transparent and responsible communication. Individual privacy will therefore be protected, and society's values will remain.

Future Directions in M2M Communication Research: We see how M2M communication forthcoming trends and challenges and in the following sections we look at emerging technologies and possible research paths. After careful

consideration of the present ones and the ones that are yet to exist, [8] this paper suggests a roadmap for future research involving M2M communication and disaster management. The study asks M2M communication as a transformative technique having potential gifts to make in emergency response capabilities, so it lays the ground for more progress in real-time communication, interoperability, and resilience.

V. METHODOLOGY

In the methodology subsection, the systemic procedure applied for research execution is presented in a form and the information was collected, preprocessed, machine learning techniques were used in addition to the framework of analysis was employed to attain the project objectives.

Data Collection:

For this research, the primary data source is the RT-IoT-2022 dataset that is used to model the normal as well as the abnormal behavior related to the TTN network environment.

It is the dissociative and integrated information set comprising the remotely accessed internet of things devices such as Thing Speak-LED, Wipro-Bulb, and MQTT-Temp, along with the simulated attack scenarios including DDoS attacks, brute-force SSH attacks, and network reconnaissance techniques [16]. The dataset considers zone-by-zone network attributes prodded into life using the Zeek network monitoring tool and Flowmeter module. It is comprised of network data captures, including from the offender's and victim's devices communicating through a router, providing the ability to observe all the extract network activities during emergency services.

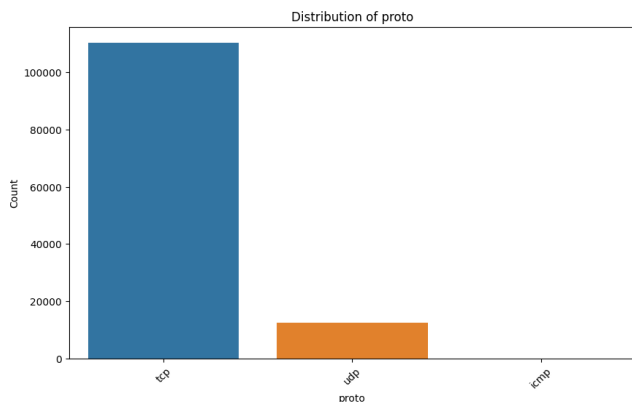


Fig. 1: Data Collection

Data Preprocessing:

The data collection phase leads to preprocessing of data through elimination of irrelevant or redundant information so that it can be used for machine learning algorithms. The step of preprocessing consists of removal of 'no' and 'Attack_type' columns from the dataset to have a precise feature set so as to ease further analysis. Similarly, relevant to positioning and categorization, 'proto' and 'service' are also coded, but with Label Encoder which is converted to a number that algorithms use. The distribution pattern of attacks is displayed throughout

the Bar charts and pie charts to investigate the imbalance class distribution, just as the correlation heat map is generated to analyze the features that are numeric across all the data set.

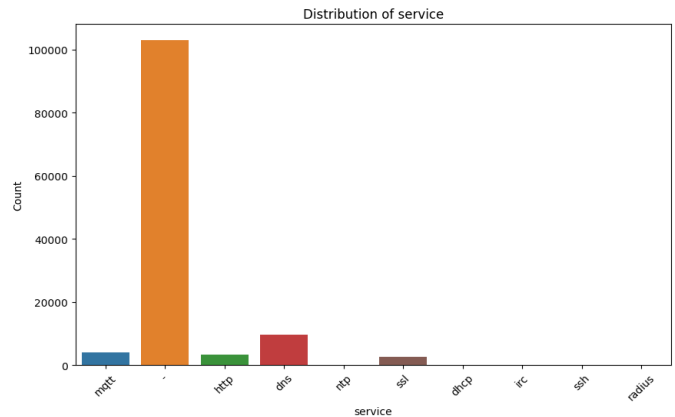


Fig. 2: Data Processing

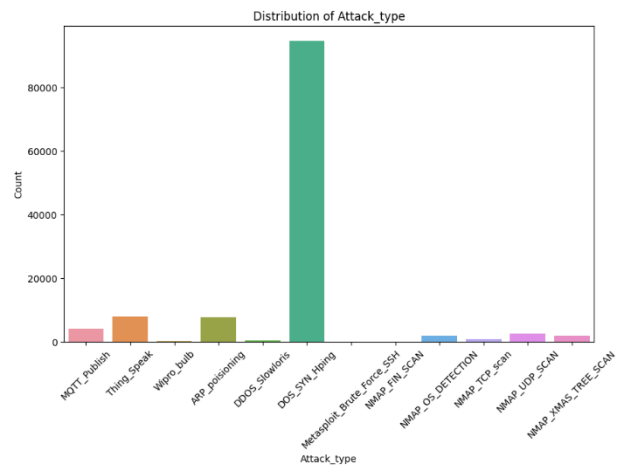


Fig. 3: Distribution of Attack_type

Pie chart of Attack Type:

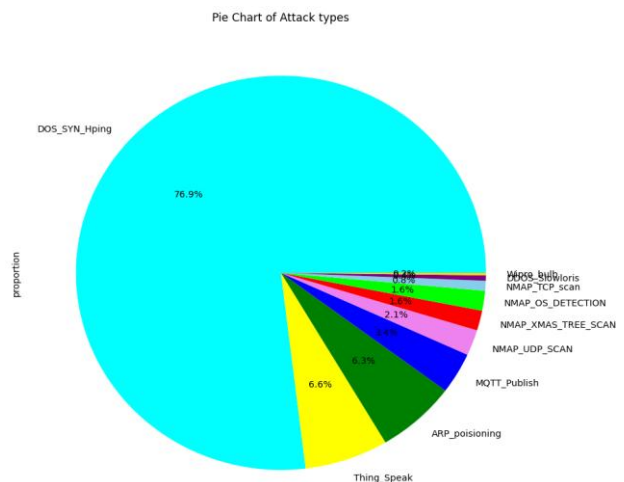


Fig. 4: Pie Chart of Attack Type

Machine Learning Techniques Used:

Machine (ML) learning techniques are utilized to shape the modeled & analyzed data that is the result of preprocessing, which includes Logistic Regression, Decision Trees using Gini Index and Entropy, Multi-Layer Perceptron (MLP) and Naïve Bayes classifier [17]. These methods among them give alternative options for classification, through which one can experiment with various modeling techniques and their efficacy on a given dataset. The Logistic Regression is a linear model that works well for the two-category classification. However, the Decision Tree method uses the Gini Index and Entropy measures to divide the feature area and subsequently make predictions. The artificial neural network MLP is good at the modeling of complex nonlinear relationships in data, meanwhile, the naïve Bayes performs the inference of non-linearity as its probability rather than raiser.

Classification	Accuracy
Logistic Regression	0.894087
Gini Index	0.997807
Entropy	0.997888
MLP	0.963288
Naive Bayes	0.863873

Fig. 5: Classification and Accuracy

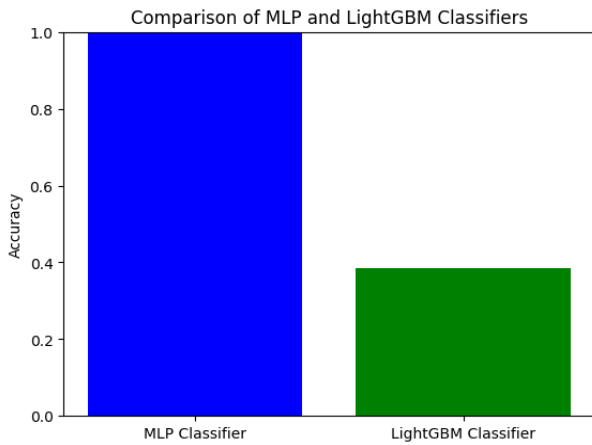


Fig. 6: Comparison of MLP and LightGBM Classifiers

Analysis of Traffic Patterns:

The study of dynamics of M2M data transmission during the emergency medical services is inevitable for the discovery of networking activity patterns and the detection of possible weak elements. This foray is an in-depth exploration of traffic patterns, including stats overview for the dataset and how to detect traffic patterns and anomalies in temporal and spatial aspects.

Overview of Dataset:

Analysis based on this foundation is on RT-IoT2022 data set which has been thoughtfully collected to have both normal and enemy behavior which happen to be in real life circumstance. With this original dataset, one can see the network traffic from every angle in the full network of emergency services. It includes both behavioral legacy data and data produced by IoT devices, like the ThingSpeak-LED, Wipro-Bulb, and the MQTT-Temp, and its architecture is designed to simulate various attack scenarios such as DDoS attacks and brute-force SSH attacks. The network monitoring tool Zeek collecting the attributes in the bidirectional format of the network traffic offers very detailed information that is suitable for dissecting the traffic nature and the situation when critical events happen.

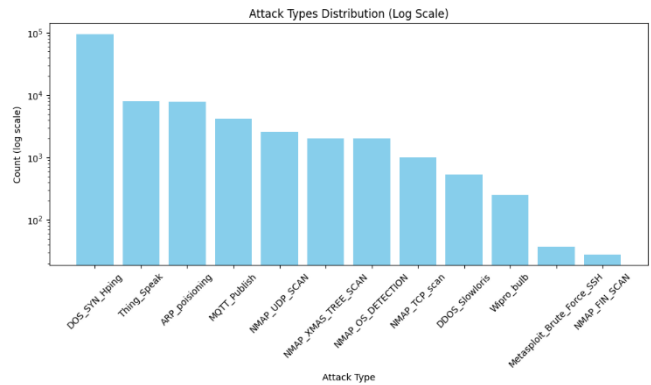


Fig. 7: Attack Types Distribution

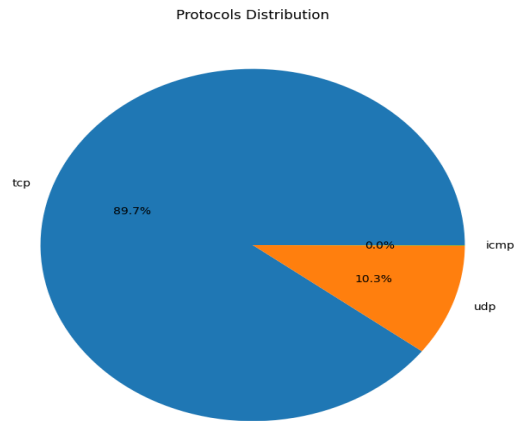


Fig. 8: Protocols Distribution

Identification of Traffic Patterns:

One of the main things one needs to do while analyzing is that he or she should look out for some patterns in the data collected from the network traffic. Through sophisticated quantifying tools and machine learning methods, abnormalities like data peak transmission are easily recognizable, as well as odd data flow patterns which are something of common triggers utilized by specific categories of web traffic. Which they correspond to the usual activity in

a network and functioning of the system just as suspects and the incidence of network attack. Via explorative data mining and pattern recognition AI tools, the study aims to disclose some of the fundamental structures of M2M network traffic of emergency communication during high-stake circumstances, deriving more details about multi-sensor automatic response services.

Anomalies Detection:

Spotting the deviations within the network traffic is while it cannot overemphasized because it prevents imminent risks from landing in the security realm and safe communication is also encouraged. Outlying cases include alterations of the already developed traffic schemes, unpredicted surge or recession of data transmission rate as well as erratic patterns of data in terms of timings and volumes. Through tools like statistical approaches, clustering techniques, and machine learning mechanisms, the research effort seeks to not only identify but categorize unusual network habits in the moment they take place [19]. The proactive approach would be to differentiate the two since the threat emanates from malicious attacks against communication infrastructure facilities with the need to introduce prompt actions in order to protect it against unanticipated disruptions.

Security Protocols and Assessment of the Possible Threats In the context of M2M (Machine-to-Machine) communication of Emergency response systems, it is essential to have a secure and high quality based transmission of data. Therein follows an essential section that conducts a thorough assessment of security and evaluation of the threat that is composed of vulnerability analysis for public safety, proposed preventive measures, and data privacy and security related ethical concerns.

Emergency Management in Vulnerability Analysis:

The rapid and risky nature of emergency services, in which all the seconds matter, involves vulnerability analysis as its integral component for having a reliable and resilient communication infrastructure in place. The evolving feature of emergency cases introduces significant obstacles that is why vulnerability exercises should be done to flush out possible weakness and solve them before they occur. One major gap during emergency help calls is the inherent openness to cyberattacks especially DDoS which are popular in the hacking circles. These attacks seek to impair the communication systems by sending a flood of nonsense traffic to jam the network and prevent mission critical systems from being used thereby hampering effective response operations. Nowadays, most emergency services use their connected devices on the Internet of Things (IoT) model, rapidly increasing the risk of DDoS attacks which security measure should be comprehensive and vulnerability assessment should be proactive [21].

Similarly, the surge of Internet of Things (IoT) gadgets in the emergency response systems adds more possible attack lanes and obscurity. IOT hardware, sensors, wearables, drones and cars, become a major part of interconnected electrical circuits communicated through diverse communication protocols. Though the heterogeneity of the IoT systems makes them vulnerable to attacks by malicious actors, there are no

prevailing standardized security protocols that can help organizations deal with this cyber threat. Sources of danger like passwords as default, firmware that is insecure and unprotected are ways through which the IoT may get attacked; in the end, this may pose a threat to integrity and availability of critical services during crucial events.

Ethical Considerations in Data Privacy and Security:

When it comes to M2M communication and emergency services in particular data privacy and security challenges are severe thus ethical adherence to personal right restrictions while holding M2M communication strong enough to ensure that the emergency response continues to be efficient. The central ethical issue linked with the data gathering, storage, and use is among the things that should be prioritized in the event of an emergency scenario [25]. On the one side, real-time data sharing is necessary for the proper resilience coordination actions, but at the same time it is important to proceed the data collection in a way that safeguards the individual privacy rights. In an emergency situation, responders must observe the rules of data saving and only gather data, the use of which will ensure the performance of the tasks given and thus the public data must be anonymized all the time. This is a guarantee for the absence of unauthorized actions of third parties.

Integration of Data Science, Telecommunications, and Emergency Management:

Imbedding data science, telecommunications and crisis management principles together creates a full framework to handle crises from a comprehension, analysis, and response point of view. Data Science is in fact a powerful tool for getting to conclusions, detecting patterns, and preventing risks by analyzing the huge amount of data from all the places where it is generated, such as sensors, social media and remote satellites. By using tools such as data mining, machine learning, and predictive analysis, Data Science enables crisis management agencies to be able to respond to events and drift in the right direction using real-time information.

The effectiveness of modern emergency telecommunications relies on the functionality of the telecommunications infrastructure, which enables the transfer of life-saving data among the responders, stakeholders, and the affected communities through mass media. The use of technological advancements of telecommunications such as mobile networks, satellites, and networked devices can be based by the emergency management organizations to build the more durable communication networks for even when the situations are undesirable. This channel of communication helps the loss of life through alerting the public to danger, explaining how to protect themselves, and providing relief and rescue based on a situation.

Collaborative Strategies for Emergency Response:

Partnership is the sphere of successful emergency response planning, though no institutions or fields covered all the facets of a complicated emergency by itself. Through strengthening cooperation among different stakeholders from the governments, non – governmental organizations

(NGOs), private sector entities, academia, and local communities, multi-sectoral approaches can be formulated to boost the strength and effectiveness of emergency response processes.

Discussion and Findings:

This is the ultimate step in our paper after which we are going to sum up all our key findings here and explore the significance of the findings based on the implications for practice and policy, and the research constraints we encountered. By carrying out an extensive investigation of the internet traffic volumes, this involves hardware and software security provisions, the analysis of different platforms and pertinent agencies, we will delve into the details of M2M communication during emergency response operations and find a solution for problems faced in the decision-making process in critical situations.

Summary of Key Findings:

The examination of internet traffic traces with provision promoting emergency service on the network showed how complicated the processes of the internet communications are from many different perspectives and how they change during the different stages of the event. Through the lens of the RT-IoT2022 dataset, we were able to dissect various types of attacks and understand the patterns that emerge when the enemy is performing attacks such as DDoS, brute-force SSH attacks, credit Chinese proverb Though, during our research we came to know that the influential properties of network traffic are on display not in one direction, but both of them; and about the importance role of the timely delivery in the error resolution services.

Implications for Practice and Policy:

The conclusion of this paper presents grave consequences and alters practice of and makes emergency management policy more effective. Concretely, these goals are best achieved using implementation of resilient security frameworks as well as of the use of advanced technologies like IoT and drones which offer the opportunity of the improvement of emergency response capability. Through training and professional development programs, improving the infrastructure and partnering with multi-agencies and disciplines, the crisis management agencies can give their fullest when it comes to saving lives in a crisis through M2M communication. Besides that, the policy-making bodies will have a basis on which they can support the proactive actions to resolve the ethic challenges and the legal issues around data privacy and security. Policy makers must establish policies that would be functioning and flexible enough to provide appropriate and required guidelines to promote technological advancements, as well as making sure that the rights of the individuals would be protected. By supporting the principles of transparency, accountability, and participation of stakeholders, civil servants can build a climate that will facilitate responsible data usage and ethical management of emergency services across all government organizations.

Limitations of the Study:

However, this one cannot be done, despite the contribution made through this, there is an issue regarding some limitations.

First, we should be aware that the data source might be only used and could be required for the generalizability of the findings in other settings or contexts with different characteristics can be limited. Moreover, the multifaceted nature of cyber threats coupled with technological advancements is a constant factor which compels researchers to obtain relevant information and utilize it to fortify their security measures. Besides, the multifaceted nature of the research yields the challenges of coordination and collaboration in collaboration among various domains, and hence the concerted approach to cut across the disciplines and gird the interdisciplinary dialogue is the requirement. Eventually, these discussions and findings presented in the paper of this research provide the light of how intricate and complex communication between M2M is like and internet traffic patterns, security measures, application analysis, and interdisciplinary approaches that will impact the current learning theories presented in the cognitive psychology are being subconsciously acquired. This model of research case study evaluation for connective resilience incorporates a summary of key findings, an exploration of the practical and policy implications, and a mention of the study limitations that will enable the future research and practical interventions in disaster communication infrastructure to improve resilience and emergency response outcomes in the ever-changing world.

VI. CONCLUSION

In this paper, we came to a deep study of Machine-to-Machine (M2M) communication that has become critical for emergency services being aware of internet traffic patterns, security measures and analyzed the applications considered in this regard and devised an interdisciplinary approach. On finishing this paper, we will outline what our research was aimed for, what has been discovered, and present our repository to the field, being, of course, open for future explorations.

Contributions to the Field: This study demonstrates that the field of emergency management and M2M communication has clearly been advanced by the knowledge we have gained. Firstly, by peeling the layers off internet traffic patterns and security measures during the time of disasters, we will be able to provide effective and intelligence reveals that pave the way for building effective protocols and strategies designed for disaster periods. Besides, we divide this section into subsections in which different applications may be covered and M2M interface should be reviewed to provide better emergency services and to have more chance for innovation and optimization of responses. Furthermore, it is the way we interweave notions of data science, telecommunications, and emergency management that allows us to comprehend complex interrelations between technology and society in the emergency service provision. Through the removal of interdisciplinary barriers and the creation of an environment that holds teamwork as the standard, we lay the foundation for M2M communication technology-based emergency

response systems that not only work, but also evolve with time to fulfill the different needs arising.

Suggestions for Future Research: Although this context offers a useful framework for the talk about M2M communication, during the emergency services, lots of fields for further research are needed. On top of that, future studies must replicate and expand the results using more relevant data from different types of environments and practical deployments. Further, will the future studies be giving rise to changing security conditions and replies to the new types of cyber threats and tech upgrades. Additionally, in the future, research needs to focus on the ethical and legal consequences of M2M communication in emergency services introducing data security, privacy, etc.

REFERENCES

- [1] Salvatore, A. (2022). AUTOSAR's transformers and MQTT for fast and secure communication between cars and external networks (Doctoral dissertation, Politecnico di Torino).
- [2] Lopez-Martin, M., Carro, B., Sanchez-Esguevillas, A., & Lloret, J. (2017). Network traffic classifier with convolutional and recurrent neural networks for Internet of Things. *IEEE access*, 5, 18042-18050.
- [3] Ji, S. Y., Jeong, B. K., & Jeong, D. H. (2021). Evaluating visualization approaches to detect abnormal activities in network traffic data. *International Journal of Information Security*, 20(3), 331-345.
- [4] Gallais, C., & Filiol, E. (2017). Critical infrastructure: Where do we stand today? A comprehensive and comparative study of the definitions of a critical infrastructure. *Journal of Information Warfare*, 16(1), 64-87.
- [5] Fukuda, K., Amaral, L. A. N., & Stanley, H. E. (2003, December). Dynamics of temporal correlation in daily internet traffic. In *GLOBECOM'03. IEEE Global Telecommunications Conference (IEEE Cat. No. 03CH37489) (Vol. 7, pp. 4069-4073)*. IEEE.
- [6] Markakis, E. K., Lykourgiotis, A., Politis, I., Dagiuklas, A., Rebahi, Y., & Pallis, E. (2017). EMYNOS: Next generation emergency communication. *IEEE Communications Magazine*, 55(1), 139-145.
- [7] Ebersold, K., & Glass, R. (2016). THE INTERNET OF THINGS: A CAUSE FOR ETHICAL CONCERN. *Issues in Information Systems*, 17(4).
- [8] Mehmood, Y., Haider, N., Imran, M., Timm-Giel, A., & Guizani, M. (2017). M2M communications in 5G: state-of-the-art architecture, recent advances, and research challenges. *IEEE Communications Magazine*, 55(9), 194-201.
- [9] De Mattos, W. D., & Gondim, P. R. (2016). M-health solutions using 5G networks and M2M communications. *IT Professional*, 18(3), 24-29.
- [10] Minoli, D. (2013). Building the internet of things with IPv6 and MIPv6: The evolving world of M2M communications. John Wiley & Sons.
- [11] Sellnow, T. L., Ulmer, R. R., Seeger, M. W., & Littlefield, R. (2008). Effective risk communication: A message-centered approach. Springer Science & Business Media.
- [12] Breuer, H., Grabowski, H., & Arnold, H. (2011). The shape of things to come: Scenarios and visual stories for telecommunication in 2020. In *Proceedings of the IADIS International Conference on Telecommunications, Networks, and Systems (Vol. 201, pp. 107-114)*.
- [13] Sharmila, B. S., & Nagapadma, R. (2023). Quantized autoencoder (QAE) intrusion detection system for anomaly detection in resource-constrained IoT devices using RT-IoT2022 dataset. *Cybersecurity*, 6(1), 41.
- [14] Burg, A., Chattopadhyay, A., & Lam, K. Y. (2017). Wireless communication and security issues for cyber-physical systems and the Internet-of-Things. *Proceedings of the IEEE*, 106(1), 38-60.
- [15] Castellano, M. B. (2004). Ethics of Aboriginal research. *International Journal of Indigenous Health*, 1(1), 98-114.
- [16] Pereira, Â. G., Benessia, A., & Curvelo, P. (2013). Agency on the Internet of Things. JRC Scientific and Policy Reports.
- [17] KASAP, P., & ZORLU, B. Ş. Ç. (2020). Classification of Factors Affecting Renal Failure by Machine Learning Methods. *Erciyes Üniversitesi Fen Bilimleri Enstitüsü Fen Bilimleri Dergisi*, 36(1), 88-101.
- [18] Mahoney, M. V., & Chan, P. K. (2002, July). Learning nonstationary models of normal network traffic for detecting novel attacks. In *Proceedings of the eighth ACM SIGKDD international conference on Knowledge discovery and data mining (pp. 376-385)*.
- [19] Bzdok, D., & Meyer-Lindenberg, A. (2018). Machine learning for precision psychiatry: opportunities and challenges. *Biological Psychiatry: Cognitive Neuroscience and Neuroimaging*, 3(3), 223-230.
- [20] Andreev, S., Galinina, O., Pyattaev, A., Gerasimenko, M., Tirronen, T., Torsner, J., & Koucheryavy, Y. (2015). Understanding the IoT connectivity landscape: a contemporary M2M radio technology roadmap. *IEEE Communications Magazine*, 53(9), 32-40.
- [21] Butun, I., Österberg, P., & Song, H. (2019). Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. *IEEE Communications Surveys & Tutorials*, 22(1), 616-644.
- [22] Sun, Y. L., Han, Z., Yu, W., & Liu, K. R. (2006, April). A trust evaluation framework in distributed networks: Vulnerability analysis and defense against attacks. In *Proceedings IEEE INFOCOM 2006. 25th IEEE international conference on computer communications (pp. 1-13)*. IEEE.
- [23] Elmustafa, S. A. A., & Mujtaba, E. Y. (2019). Internet of things in smart environment: Concept, applications, challenges, and future directions. *World Scientific News*, 134(1), 1-51.
- [24] Mazurczyk, W., Wendzel, S., Zander, S., Houmansadr, A., & Szczypiorski, K. (2016). Information hiding in communication networks: fundamentals, mechanisms, applications, and countermeasures. John Wiley & Sons.
- [25] Silva, R., & Iqbal, R. (2018). Ethical implications of social internet of vehicles systems. *IEEE Internet of Things Journal*, 6(1), 517-531.
- [26] Gállego, J. R., Hernández-Solana, Á., Canales, M., Lafuente, J., Valdovinos, A., & Fernández-Navajas, J. (2005). Performance analysis of multiplexed medical data transmission for mobile emergency care over the UMTS channel. *IEEE transactions on information technology in biomedicine*, 9(1), 13-22.
- [27] Menon, V., Arjun Rathya, R., Prasad, A., Gopinath, A., Sai Shibu, N. B., & Gayathri, G. (2021). Exploring iot-enabled multi-hazard warning system for disaster-prone areas. In *Advances in Computing and Network Communications: Proceedings of CoCoNet 2020, Volume 1 (pp. 405-422)*. Springer Singapore.
- [28] Schooley, B., Abed, Y., Murad, A., Horan, T. A., & Roberts, J. (2013). Design and field test of an mHealth system for emergency medical services. *Health and Technology*, 3, 327-340.