SIoTSim: Simulator for Social Internet of Things

Meriem Chiraz Zouzou, mohamed Shahawy, Elhadj Benkhelifa and Hisham Kholidy

November 16, 2023

SIoTSim: Simulator for Social Internet of Things

Meriem Chiraz Zouzou[1], Mohamed Shahawy[1], Elhadj Benkhelifa[1] and Hisham Kholidy[2]

[1] Smart Systems, AI and Cybersecurity Research Centre, Staffordshire University, UK
[2]SUNY Polytechnic Institute, Utica USA
e.benkhelifa@staffs.ac.uk

***Abstract*—Abstract— The Social Internet of Things (SIoT) concept extends beyond the Internet of Things (IoT) by integrating principles from social networking to form interconnected networks of intelligent objects. This integration enables the creation of smart objects that can interpret and react to human needs and requirements, resulting in an enhanced interactive encounter. However, the complex nature of these systems presents challenges when it comes to validating their effectiveness and performance in various real-life scenarios. To overcome this challenge, this paper introduces a novel simulator called SIoTSim that provides complex simulation functionalities and presents different SIoT relationships, including Human to Human, Object to Object, and Human to Object relationships. Additionally, the simulator also models the behaviour of SIoT systems in different contexts to create realistic SIoT datasets, taking into account various contextual factors, such as user behaviour, interactions within social networks, and device characteristics. By using SIoTSim, researchers and developers can effectively assess and analyse the performance of their SIoT systems. The insights gained from the simulation results could guide decision-making processes and facilitate the development of more efficient and reliable SIoT systems that are better suited to meet the needs of users in different contexts .**

Keywords—Social IoT, IoT, Simulation, Synthetic Data, Trust Management, Dataset

I. Introduction

The rapid advancements in communications and computing have led to the emergence of various technologies that collectively support a network of intelligent and interconnected objects. This ecosystem can be described in diverse ways, IoT and Machine to Machine Communication (M2M). As a result, the implementation of intelligent features, whether integrated within devices themselves or provided through cloud-based storage and processing, has turned the long-standing vision of machine intelligence into a tangible reality. Over the past years, researchers have extensively discussed the idea that enriching communication in IoT ecosystem with concepts and aspects from Social Networks (SN) enhances the potential of connected devices. This approach aims to provide more meaningful and interpretable interactions for the benefit of end-users [1]. This convergence gives rise to the concept of the Social Internet of Things (SIoT), which constructs a social network of interconnected intelligent objects. While IoT follows two interaction paradigms, human-to-human (H2H) and thingto-thing (T2T), SIoT adds human-to-thing (H2T) interactions. Objects in SIoT are able to interact similarly to humans, based on different types of relationships [1] [2] [3]. The initial phase of socialisation that contributes to the formation of a parental object relationship (POR) is consistent among objects produced simultaneously by the same manufacturer. This form of relationship will not change with time but can be updated by a distributed event. The co-worker object relationship (COR) refers to objects collaborating in shared experiences, such as work, to achieve common objectives, but only within specific locations like offices or laboratories. A co-location object relationship (LOR) emerges when objects share individual experiences, typically based on location. Both co-location and co-worker relationships are subject to change over time and in response to interaction frequency and reputation. Objects sharing the same owner establish an Owner-object relationship (OOR). Lastly, the social object relationship (SOR) pertains to objects that sporadically or consistently come into contact and are inherently associated with their owners. The nature of this relationship hinges on planned interactions managed by owners, influencing whether these objects evolve into friends or remain strangers [4]. In SIoT, objects take some capacity from humans and mimic their behaviours when searching for new friends. After an owner defines the rules, an object builds and manages several types of relationships and applies them to navigate the network searching for services [5]. The SIoT brings added value to users by facilitating more effective navigation, service discovery, trustworthiness, and other benefits. However, the complexity of these systems makes it challenging to validate their effectiveness and performance under different real-world conditions. To address this challenge, this paper introduces a simulation tool called SIoTSim that represents the social relationships of an entity in SIoT. The primary objective of the SIoTSim is to simulate and analyse the behaviour of SIoT systems such as devices, sensors, and users in different SIoT contexts, enabling the generation of realistic SIoT data for testing and evaluation. Moreover, SIoTCim offers flexibility and adaptability, allowing the customisation of various simulation parameters to produce tailored synthetic data. It incorporates a range of functionalities, including the simulation of different sensors and networks, as well as the modelling of various attacks and vulnerabilities. The remaining sections of the paper are organised as follows: Section II provides an overview of the current state of SIoT simulators, section III offers a detailed description of SIoTSim, Section IV presents the possible scenarios that can be simulated using

SIoTSim Finally, Section V concludes the paper, and outlines future research directions.

II. RELATED WORK

As the SIoT paradigm gains more attention in research, it is important to find appropriate simulation tools to design a specific SIoT environment that incorporates the social structure of objects. While there are various simulation tools available for the IoT environment, such as OMNET++, NS2, and Cooja, not all of them are suitable for addressing the complexity of the social structure of objects in the SIoT environment [6]- [7]. This section focuses on the simulation tools, which can specifically be related to SIoT. The literature frequently employs several simulation tools for this purpose, which are summarised in Table 1 and discussed below.

Osterlind et al. introduced a simulator named COOJA, designed for cross-level simulation using the Contiki sensor node operating system [8]. This simulator enables concurrent simulations at multiple levels, including the network level, the operating system level, and the machine code instruction set level. Cooja allows researchers to analyse the performance and behaviour of their WSN designs in a simulated environment before deployment in real-world scenarios. Varga et al. put forward a simulator known as OMNeT++ specifically designed for low-level peer-to-peer communication networks, focusing on optical switches and stored networks [9]. OMNET++ is a commonly used discrete event simulation tool in sensor network research. It is a well-established and comprehensive tool that can be used to integrate external factors to meet specialised environmental requirements. For example, OMNET++ can incorporate mobility for vehicular networks and include social profiles of objects to enhance application capabilities [10]. Generally, due to its flexibility, OMNET++ can be used in various domains and applications. SWIM was initially introduced as a mobility model for ad-hoc networking and is capable of producing synthetic traces of mobility patterns to create a small world. Additionally, SWIM is designed to consider social behaviour similar to that of humans in reallife scenarios. Moreover, statistical analysis has shown that the synthetic traces generated by SWIM are quite similar to those of humans [11]. Henderson et al. introduced a simulator framework known as ns3. This framework is designed to consume network packets by utilising real device drivers or VLANs [12]. NS- 3 is an open-source discrete-event simulator that is considered to be the successor of NS-2. It is a versatile tool that can be used to create simulation scenarios that closely resemble real-world devices and protocols. Due to its adaptability and flexibility, NS-3 is a popular choice for network simulation across various fields and applications [13] [14]. There are many other simulation tools available besides the ones discussed previously that have been used by researchers to simulate the SIoT environment. These include Python, and Microsoft Visual Studio. Researchers used Python as a simulation environment, especially for prediction-based studies. Kasnesis et al. introduced a simulator named ASSIST, which focuses on agent-based semantic rules and services specifically designed for SIoT applications [15]. Abderrahim et al. introduced a simulator named TMCoT-SIoT, which is a trust management system that utilises community interest to mitigate on-off attacks [16]. Defiebre et al. developed a simulator known as DANOS, which aims to enhance object profiles and their interaction behaviour by incorporating intelligent features like human friendships [17]. Recently Gazi et al. focused on developing a SIoT simulator to address traffic congestion issues in urban areas through a monitoring traffic control system [18].

III. SIOTSIM: SIMULATOR IN SIOT

SIoT refers to a network of diverse IoT devices that collaborate to create an intelligent ecosystem, aiming to assist users in their tasks. These devices interact with each other based on predefined relationships, mimicking the structures found in social networks. Therefore, SIoTSim illustrates the capabilities of the system in facilitating autonomous relationships among SIoT objects. These relationships allow the objects to exchange best recommendations with each other and their respective owners. Additionally, the SIoTSim simulates and analyses the behaviour of SIoT systems such as devices and users in different SIoT contexts, enabling the generation of realistic SIoT data for testing and evaluation. Some modelled functionalities that take part in the simulation process include (i) forming friendships between users, (ii) users joining Communities of Interest (CoIs; i.e. social groups), (iii) devices dropping connections and leaving the network, (iv) users probabilistically communicating (individually, multicast as part of a CoI, or broadcast to all their connections), and (v) stochastic malware propagation across the network. The simulator has been implemented using Python and deployed on Google Colab to facilitate cross-platform access, provide a user-friendly interface to configure the tool as needed and enable on-demand computational resources.

A. SIoTSim design

The simulated network is represented as a NetworkX MultiDirected Graph (MultiDiGraph) to capture bilateral relationships between entities. Additionally, the simulation process is based on generic timesteps to capture the functionalities' temporal qualities. SIoTSim consists of 2 key high-level modules: Nodes and Events.

1) Nodes module: A Node is modelled as an abstract class that represents any entity (namely Users and Devices) within the simulation graph. It does not directly represent a specific node in the graph, but rather provides a shared set of attributes and behaviours across all entities in the graph. Each node in the simulation graph shares the following attributes:

TABLE I
EXISTING NETWORK-SIMULATION TOOLS

Ref	Simulators	Languages	Scope	Mobility	Cyber-attacks simulation	Overall practical
[8]	Cooja	C/Java	Network	Yes	Incorporated custom Extensions	Significant
[9]	OMNeT++	C++	Network	Yes	Incorporated custom Extensions	Average significance
[12]	NS-3	C++	Network	Yes	No	Significant
[15]	ASSIST	NA	SIoT	No	No	Low significance
[16]	TMCoT-SIoT	Python	SIoT	No	No	Low significance
[17]	DANOS	Go 1.12	SIoT	No	No	Low significance
[18]	Traffic simulator	C	SIoT	No	NA	Low significance

- Trust Value: This attribute denotes the level of trust that other nodes in the graph have towards this particular node. It is likely used to determine the interactions and relationships with other nodes.
- Connection Status: This attribute indicates the connectivity status of the node to the network. This attribute is automatically set to true for the user's node when at least one of their devices is connected to the network. It is used to determine which nodes can communicate with each other.
- Node ID: This attribute serves as a unique identifier for the node. It can be manually assigned during instantiation or automatically generated in a sequential manner. The ID attribute plays a crucial role in identifying nodes within the simulation graph.
- Connections Established: This attribute is a list that contains the connections to other nodes of the same type. In other words, a user node can only be connected to other User nodes, and a Device node can only be connected to other Device nodes.

2) Events module: Similar to Nodes, Events are also modelled with a layer of virtualisation to capture the shared set of attributes and functionalities. The fundamental structure of an Event is abstracted from a Pandas [19] Series, where each row contains: (i) the timestep, (ii) the type of event (expanded upon in Table 2), (iii) source device ID,

(iv) source device's owner ID, (v) destination device ID, (vi) destination device's owner ID, and lastly (vii) the event's payload content. There are 4 high-level types of Events in SIoTSim that capture all types of transactions. Some repeated events within a single timestep indicate particular forms of functionalities. For instance, joining a CoI would be simulated as multiple simultaneous DEVICE HANDSHAKE events. Similarly, multicast and broadcast messages are modelled as concurrent P2P messages.

B. SIOTSIM Stochastic Event Allocation

As depicted in Figure 1, all simulated events are triggered probabilistically based on a custom probability density function derived from the Gaussian distribution (Equation 1).

$$P = \frac{\beta\sigma}{\sigma\sqrt{2\pi}} exp(-\frac{1}{2} - \frac{(x-\mu)^2}{\sigma^2}) \quad (1)$$

Where $x = timestep$, $\mu = 0$, and $\sigma = \frac{100}{3}$, which estimates 99.7% of the values to fall within the [-100,100] range according to the 68–95–99.7 rule. The resulting sampling value is then truncated to the aforementioned preset range to account for the 0.3% outliers.

The additional term β is a scaling factor (bounded to [0.5, 2.5], inclusive) for the density function that controls the range amplification and how steeply the function diminishes to 0.

Basing Event likelihood on P (or$P_{complement} = 1 - P$) ensures that certain events are more likely to occur at the beginning of the simulation (such as users joining the network and devices activating), while others tend to occur later (such as messaging between users and join Communities of Interest).

By incorporating realistic timing and probability distributions for different event types, the simulation aims to accurately replicate real-world behaviours. Regarding device initialisation, a deliberate effort is made to interleave malicious and trusted devices instead of concatenating them sequentially. This design choice ensures that the initial network topology reflects a real-world scenario where malicious and trusted devices are randomly scattered throughout the network, rather than being grouped together. The simulation environment closely resembles real-world dynamics and enhances the fidelity of the simulation results.

C. SIoTSim parameters

SIoTSim serves as a valuable tool for replicating the actions and behaviours of devices in diverse scenarios within SIoT environment. To ensure an accurate emulation of these nodes, SIoTSim commonly utilises a predefined set of parameters, as outlined in the accompanying table. These parameters play a pivotal role in defining the unique characteristics and attributes of the system under simulation. By carefully configuring and adjusting these parameters, SIoTSim can recreate various SIoT scenarios, allowing researchers and developers to analyse and optimise system performance, behaviour, and interactions within the SIoT network.

TABLE II
VENT TYPES

Event Type	Description
DEVICE_JOINED_NETWORK	Indicates when a device has joined the network
DEVICE_LEFT_ NETWORK	Indicates when a device has disconnected from the network
DEVICE_ HANDSHAKE	Triggered when 2 devices connect
DEVICE _P2P _MESSAGE	Triggered when transmission occurs between 2 devices

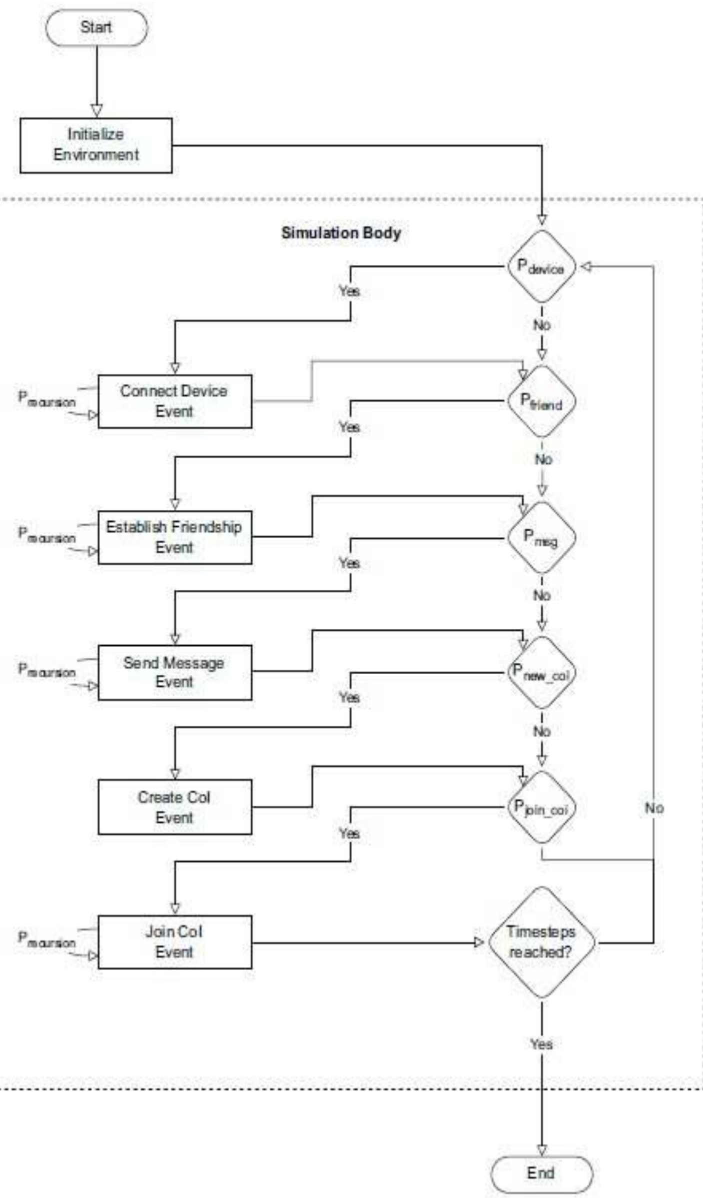

Fig. 1. IoTSim Flowchart

IV. SIOTSIM SCENARIOS

TABLE III
IMULATOR PARAMETERS

Parameters	Definitions
SIMULATION_TIME_STEPS	Total number of simulation time steps
INITIAL_RECURRENCE_PROB	The initial probability of event recurrence within the same time step (i.e., two devices join the network concurrently; 0.0 = deactivated)
RECUR-RENCE_ADJUSTMENT_FACTOR	Adjustment factor of the recurrence probability (e.g., 0.5 => probability halves every recurrence)
USER_COUNT	Number of users (must be less than or equal to (DEVICES_COUNT)
FRIENDSHIP_PROB	Probability of friendship occurrence across the network (compounded with p_complement)
FRIENDLESS_PROB	Probability of users not establishing any connections (island nodes)
MIN_DEVICES_COUNT	Minimum number of devices per user
MAX_DEVICES_COUNT	Maximum number of devices per user
OTHER_DEVICES_JOIN_PROB	Probability an existing user would connect their other devices to the network
INITIAL_MALICIOUS_RATIO	The ratio of malicious devices
PREACTIVATE_DEVICES	Whether to have devices join the network at random intervals or have them pre-activated at the start
DEVICE_ACTIVATION_PROB	Probability of a device joining the network (Compounded with p)
BROADCAST_PROB	Broadcast messaging probability (p2p = 1- BROADCAST_PROB)
MAL-WARE_PROPAGATION_RATE	The rate at which a malicious device could turn another device's trust value
BROADCAST_COI_PROB	Probability of broadcasting to a COI (complement of this value is prob. of broadcasting to all connections)
COI_SPAWN_RATE	Community of Interest (CoI) spawn rate (probability of establishment – compounded with p_complement)
COI_INITIAL_PERC	Community of Interest (CoI) initial users join the rate (Percentage of the entire network)
COI_JOIN_PROB	Probability of joining an existing CoI (compounded with p_complement)
VERBOSE	An option to print extended information on each event as they are simulated

SIoTSim is specifically engineered to replicate intricate SIoT environments. Within this representation, blue nodes symbolise users, while green nodes represent a diverse range of devices encompassing sensors, smartphones, and more. The essential network connections between users are depicted by black lines, while grey lines denote connections between device owners and their respective devices, as well as deviceto-device connections. What distinguishes SIoTSim is its inherent capacity to model a multitude of diverse scenarios, such as Single-device scenario, Disconnected device scenario, Multi-user scenario. These scenarios serve as comprehensive templates, allowing for precise modelling of various SIoT environments. Depending on the research objectives and the specific dynamics under investigation. Each scenario encapsulates unique configurations, interactions, and device ownership patterns, affording a robust framework for conducting comprehensive SIoT simulations. Consequently, these diverse scenarios can be harnessed to generate extensive SIoT datasets, tailoring the simulation to reflect various factors such as the number of devices owned by users and the intricate behaviours exhibited by these devices within the SIoT ecosystem. This flexibility empowers researchers to tailor their simulations precisely to the desired context and gain deeper insights into the behaviour and performance of SIoT systems under different conditions.

Within Figure 2, a spectrum of simulation scenarios is thoughtfully displayed, each encompassing distinct characteristics and attributes. These variations serve as illustrative examples of the versatile capabilities offered by SIoTSim in simulating a diverse range of scenarios within the SIoT environment:

In the first scenario (Figure 3.A), each user owns only one IoT device that is connected to the SIoT network. This is a simple and straightforward way to collect data about IoT devices. It is often used in the early stages of development when researchers are trying to understand the behaviour of a single device. The dataset generated from this scenario would primarily focus on the behaviour of a single device such as its performance and connectivity. Moreover, the data collected from this scenario can be used to improve the performance and reliability of the device. Alternatively, (Figure 3.B) each user owns multiple IoT devices that are connected to the SIoT network. This scenario is more complex than the single-device scenario, but it is necessary to understand the interactions between devices in order to design reliable SIoT systems. The dataset generated from this scenario would focus on the behaviour of multiple devices including how they interact with each other, how they are used by the user, and their performance in addition, improve the performance and reliability of the devices or the system. In (Figure 3.C) IoT devices occasionally disconnect from the network due to various reasons such as low battery, network interference, or other technical issues. The resulting dataset encompasses crucial data regarding the

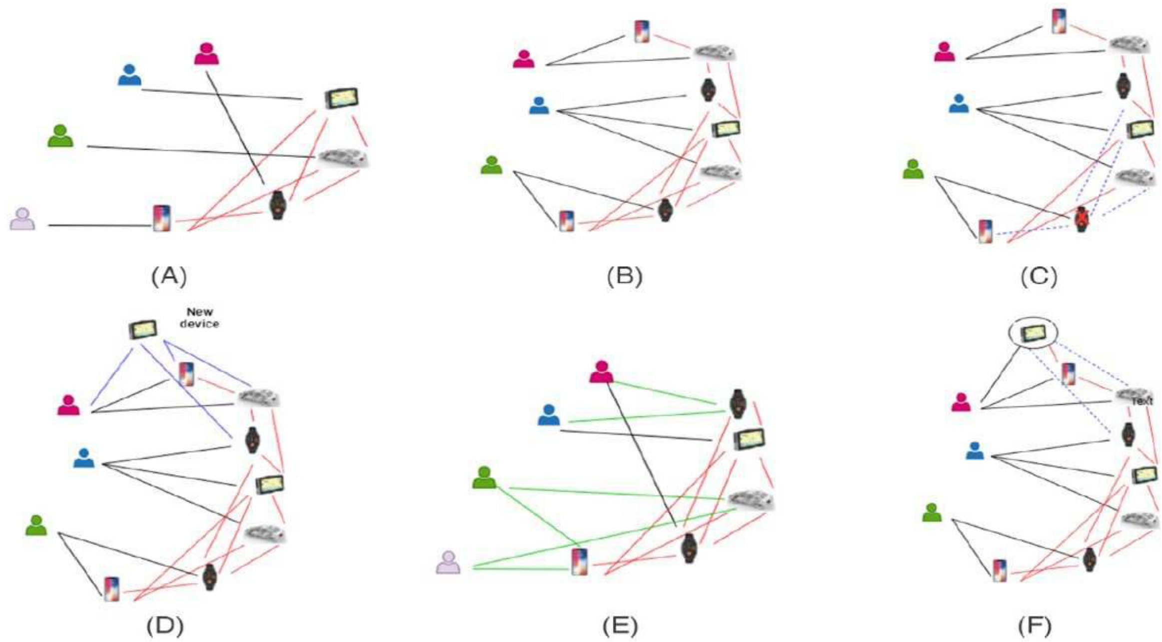

Fig. 2. IoTSim various custom scenarios

frequency and duration of these device disconnections which includes information on the frequency and duration of device disconnections as well as the impact of those disconnections on user behaviour and network performance. This scenario provides valuable insights into the reliability and robustness of SIoT systems when faced with intermittent device connectivity issues. Another scenario (Figure 3.D) portrays new IoT devices are added to the SIoT network by users. The dataset generated from this scenario would focus on the process of adding new devices to the network including the types of devices being added, the frequency of device additions, and the impact of those additions on the overall network performance and behaviour. Moreover, it is important to note that this dataset also contributes to enhancing the scalability of SIoT systems, as it offers valuable insights into the network's capacity to accommodate and adapt to the introduction of additional devices by users. Moreover, (Figure 3.E) models a relationship where multiple users share the same IoT devices or connect their own devices to the SIoT network. The dataset generated from this scenario can help evaluate the network's ability to handle multiple users and their interactions with the network as well as identify potential issues related to privacy and security. Furthermore, this dataset offers a comprehensive perspective on the SIoT environment's scalability and resilience in the face of collaborative and diverse user activities, in (Figure 3.F) the focus lies on the intermittent malfunctioning or provision of faulty data by IoT sensors within the SIoT system. The dataset produced from this scenario serves a crucial purpose in assessing the network's competence in identifying and remedying sensor faults. Moreover, this dataset offers valuable insights into the system's ability to maintain data integrity, ensuring reliable and high-quality information within the SIoT environment. IoT sensors occasionally malfunction or provide faulty data.

V. Conclusion and Future Direction

In this paper, we present a novel simulation tool in SIoT called SIoTSim. SIoTSim is a powerful and flexible tool that can help researchers and developers optimise and improve SIoT systems in different contexts. By simulating and analysing the behaviour of SIoT users and devices, SIoTSim generates insights and patterns that could be used to design and deploy more efficient and effective SIoT systems in the future. Some limitations currently identified in our tool include: (i) lack of geolocation modelling, (ii) enhanced customisation for social groups (i.e., representing coworker relationships, etc.), and (iii) statistically dependent event across time-steps.

Nevertheless, SIoTSim fills a critical gap in the Social IoT area, where existing simulation tools are either platform dependent, lack important functionality, or require substantial development to build custom extensions. Furthermore, we open-source the simulator for further research and development and provide a user-friendly Google Colab interface for easy-access.

For future work, we plan to extend our current research work with the security solutions introduced in [21-95].

References

[1] L. Atzori, “The Social Internet of Things (SIoT) - When social networks meet the Internet of Things: Concept, architecture and network characterization,” Computer Networks, vol. 56, 2012.

[2] S. Alam, “Trust Management in Social Internet of Things (SIoT): A Survey,” IEEE Access, vol. 10, pp. 108924–108954, 2022.

[3] W. Z. Khan, “Trust Management in Social Internet of Things: Architectures, Recent Advancements, and Future Challenges,” JIoT, vol. 8, no. 10, pp. 7768–7788, 2021.

[4] F. Amin, A. Ahmad, and G. S. Choi, “Towards Trust and Friendliness Approaches in the Social Internet of Things,” Applied Sciences, vol. 9, no. 1, pp. 166–166, 2019.

[5] M. Nitti, L. Atzori, and I. P. Cvijikj, “Friendship Selection in the Social Internet of Things: Challenges and Possible Strategies,” IEEE Internet of Things Journal, vol. 2, no. 3, pp. 240–247, 2015.

[6] C. Perera, “Context Aware Computing for The Internet of Things: A Survey,” IEEE Commun. Surv. Tutorials, vol. 16, no. 1, pp. 414–414, 2014.

[7] M. Chernyshev, “Internet of Things (IoT): Research, Simulators, and Testbeds,” Internet of Things (IoT): Research, Simulators, and Testbeds, vol. 5, pp. 1637–1647, 2018.

[8] A. Dunkels et al., “Cross-Level Sensor Network Simulation with COOJA,” and others, Ed.

[9] A. Varga, “omnet++,”Modeling and tools for network simulation,” and others, Ed., vol. pp. 35–59, 2010.

[10] P. Deshpande, “M4M: A model for enabling social network based sharing in the internet of things,” 2015. [Online]. Available: https://ieeexplore.ieee.org/document/7098685

[11] A. Mei and J. Stefa, “SWIM: A simple model to generate small mobile worlds,” and others, Ed., 2009.

[12] T. R. Henderson, “Network Simulations with the ns-3 Simulator 3. ADDITIONAL AUTHORS,” Proceedings of the 2003 Winter Simulation Conference, 2003.

[13] L. Campanile, “Computer Network Simulation with ns-3: A Systematic Literature Review,” Electronics, vol. 9, no. 2, pp. 272–272, 2020.

[14] H. Al-Hamadi and I. R. Chen, “Trust-Based Decision Making for Health IoT Systems,” JIoT, vol. 4, no. 5, pp. 1408–1419, 2017.

[15] P. Kasnesis, “ASSIST: An agent-based SIoT simulator,” 2016.

[16] O. B. Abderrahim, M. H. Elhdhili, and L. Saidane, “TMCoISIOT: A trust management system based on communities of interest for the social internet of things,” 2017. [Online]. Available: https://ieeexplore.ieee.org/document/7986378

[17] D. Defiebre, D. Sacharidis, and P. Germanakos, “A decentralized recommendation engine in the social internet of things,” 2020. [Online].

[18] Available: http://dl.acm.org/citation.cfm?id\&\#61

[19] S. M. Gazi and S. R. Arko, “Developing a SIoT compatible novel traffic simulator to evaluate and execute complex SIoT based algorithms in typical road traffic scenarios,” and others, Ed., 2021.

[20] W. Mckinney, “Data Structures for Statistical Computing in Python,” Proceedings of the Python in Science Conference, 2010.

[21] A. A. Khalil, M. A. Rahman and H. A. Kholidy, "FAKEY: Fake Hashed Key Attack on Payment Channel Networks," 2023 IEEE Conference on Communications and Network Security (CNS), Orlando, FL, USA, 2023, pp. 1-9, doi: 10.1109/CNS59707.2023.10288911.

[22] Hisham A. Kholidy, Fabrizio Baiardi, A. Azab, "A Data-Driven Semi-Global Alignment Technique for Masquerade Detection in Stand-Alone and Cloud Computing Systems", is Submitted in ", granted on January 2019, US 20170019419 A1.

[23] Hisham A. Kholidy, “Accelerating Stream Cipher Operations using Single and Grid Systems”, US Patent and Trademark Office (USPTO), April 2012, US 20120089829 A1.

[24] Hisham Kholidy, “Multi-Layer Attack Graph Analysis in the 5G Edge Network Using a Dynamic Hexagonal Fuzzy Method”, Sensors 2022, 22, 9. https://doi.org/10.3390/s22010009. (IF: 3.576).

[25] Hisham Kholidy, “Detecting impersonation attacks in cloud computing environments using a centric user profiling approach”, Future Generation Computer Systems, Volume 117, issue 17, Pages 299-320, ISSN 0167-739X, https://doi.org/10.1016/j.future.2020.12.009, (IF: 7.307). April 2021, https://www.sciencedirect.com/science/article/pii/S0167739X20330715

[26] Hisham Kholidy, “Autonomous Mitigation of Cyber Risks in Cyber-Physical Systems”, Future Generation Computer Systems, Volume 115, February 2021, Pages 171-187, ISSN 0167-739X, (IF: 7.307) DOI: https://doi.org/10.1016/j.future.2020.09.002 https://www.sciencedirect.com/science/article/pii/S0167739X19320680

[27] Hisham A. Kholidy, “An Intelligent Swarm based Prediction Approach for Predicting Cloud Computing User Resource Needs”, the Computer Communications Journal, Feb 2020 (IF: 5.047). https://authors.elsevier.com/tracking/article/details.do?aid=6085&jid=COMCOM&surname=Kholidy

[28] Hisham A. Kholidy, “Correlation Based Sequence Alignment Models for Detecting Masquerades in Cloud Computing”, IET Information Security Journal, DOI: 10.1049/iet-ifs.2019.0409, Sept. 2019 (IF: 1.51) https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2019.0409

[29] I. Elgarhy, M. M. Badr, M. Mahmoud, M. M. Fouda, M. Alsabaan and Hisham A. Kholidy, "Clustering and Ensemble Based Approach For Securing Electricity Theft Detectors Against Evasion Attacks", in IEEE Access, January 2023, doi: 10.1109/ACCESS.2023.3318111. (IF: 3.55).

[30] Mustafa, F.M., Hisham A. Kholidy, Sayed, A.F. et al. “Backward pumped distributed Raman amplifier: enhanced gain”, Optical Quantum Electron 55, 772 (2023). https://doi.org/10.1007/s11082-023-05066-3 (IF: 3.0).

[31] Alahmadi TJ, Rahman AU, Alkahtani HK, Hisham A. Kholidy “Enhancing Object Detection for VIPs Using YOLOv4_Resnet101 and Text-to-Speech Conversion Model”, Multimodal Technologies and Interaction. 2023; 7(8):77. https://doi.org/10.3390/mti7080077 (IF: 3.17).

[32] Alkhowaiter, M.; Hisham A. Kholidy.; Alyami, M.A.; Alghamdi, A.; Zou, C, “Adversarial-Aware Deep Learning System Based on a Secondary Classical Machine Learning Verification Approach”. Sensors 2023, 23, 6287. https://doi.org/10.3390/s23146287 (IF: 3.9).

[33] Badr, Mahmoud M., Mohamed I. Ibrahem, Hisham A. Kholidy, Mostafa M. Fouda, and Muhammad Ismail. 2023. "Review of the Data-Driven Methods for Electricity Fraud Detection in Smart Metering Systems" Energies 16, no. 6: 2852. 2023 (IF: 3.25). https://doi.org/10.3390/en16062852

[34] A Jakaria, M. Rahman, M. Asif, A. Khalil, Hisham Kholidy, M. Anderson, S. Drager, "Trajectory Synthesis for a UAV Swarm Based on Resilient Data Collection Objectives," in IEEE Transactions on Network and Service Management, 2022, doi: 10.1109/TNSM.2022.3216804. (IF: 4.75). https://ieeexplore.ieee.org/document/9928375?source=authoralert

[35] Mustafa, F.M., Hisham Kholidy., Sayed, A.F. et al., “Enhanced dispersion reduction using apodized uniform fiber Bragg grating for optical MTDM transmission systems”.

Optical and Quantum Electronics 55, 55 (December 2022). https://doi.org/10.1007/s11082-022-04339-7 . (IF: 2.79).

[36] Hisham A. Kholidy, Abdelkarim Erradi, "VHDRA: A Vertical and Horizontal Dataset Reduction Approach for Cyber-Physical Power-Aware Intrusion Detection Systems", SECURITY AND COMMUNICATION NETWORKS Journal (IF: 1.968), March 7, 2019. vol. 2019, 15 pages. https://doi.org/10.1155/2019/6816943.

[37] Hisham A. Kholidy, Abdelkarim Erradi, Sherif Abdelwahed, Fabrizio Baiardi, "A risk mitigation approach for autonomous cloud intrusion response system", in Journal of Computing, Springer, DOI: 10.1007/s00607-016-0495-8, June 2016. (IF: 2.42).

[38] Hisham A. Kholidy, Fabrizio Baiardi, Salim Hariri, "DDSGA: A Data-Driven Semi- Global Alignment Approach for Detecting Masquerade Attacks", in IEEE Transactions on Dependable and Secure Computing, DOI 10.1109/TDSC.2014.2327966, May 2014. (ISI Impact factor: 6.791).

[39] Hisham A. Kholidy, Hala Hassan, Amany Sarhan, Abdelkarim Erradi, Sherif Abdelwahed, "QoS Optimization for Cloud Service Composition Based on Economic Model", Book Chapter on the Internet of Things. User-Centric IoT, 2015, Volume 150 ISBN : 978- 3-319-19655-8

[40] Atta-ur Rahman, Maqsood Mahmud, Tahir Iqbal, Hisham Kholidy, Linah Saraireh, et al "Network anomaly detection in 5G networks", The Mathematical Modelling of Engineering Problems journal, April 2022, Volume 9, Issue 2, Pages 397-404. DOI 10.18280/mmep.090213

[41] Hisham A Kholidy., et al. "A Survey Study For the 5G Emerging Technologies", Acta Scientific Computer Sciences 5.4 (2023): 63-70, DOI: 10.13140/RG.2.2.22308.04485.

[42] Hisham A. Kholidy, Fabrizio Baiardi, Salim Hariri, Esraa M. ElHariri, Ahmed M. Youssouf, and Sahar A. Shehata, "A Hierarchical Cloud Intrusion Detection System: Design and Evaluation", in International Journal on Cloud Computing: Services and Architecture (IJCCSA), November 2012. DOI 10.5121/ijccsa.2012.2601

[43] Hisham A. Kholidy, Alghathbar Khaled s., "Adapting and accelerating the Stream Cipher Algorithm RC4 using Ultra Gridsec and HIMAN and use it to secure HIMAN Data", Journal of Information Assurance and Security (JIAS), vol. 4 (2009)/ issue 4,pp 274,tot.pag 283, 2009. http://www.mirlabs.org/jias/vol4-issue6.html

[44] Hisham A. Kholidy, "A Smart Network Slicing Provisioning Framework for 5Gbased IoT Networks", The 10th International Conference on Internet of Things: Systems, Management and Security (IOTSMS 2023). San Antonio, Texas, USA. October, 2023.

[45] Hisham A. Kholidy, "Towards A Scalable Symmetric Key Cryptographic Scheme: Performance Evaluation and Security Analysis", IEEE International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, May 1-3, 2019. https://ieeexplore.ieee.org/document/8769482.

[46] Hisham A. Kholidy, "A Study for Access Control Flow Analysis With a Proposed Job Analyzer Component based on Stack Inspection Methodology", the 2010 10th International Conference on Intelligent Systems Design and Applications (ISDA), pp 1442-1447, Cairo, Egypt, vol. IEEE Catalog Number: CFP10394-CDR, 2010.

[47] Hisham A. Kholidy, "HIMAN-GP: A Grid Engine Portal for controlling access to HIMAN Grid Middleware with performance evaluation using processes algebra", The 2nd International Conference on Computer Technology and Development ICCTD, pp 163-168, Cairo, 2010.

[48] R. Bohn, A. Battou, B. Choi, R. Chaparadza, S. Song, T. Zhang, T. Choi, Hisham A. Kholidy, M. Park, S. Go, "NIST Multi-Domain Knowledge Planes for Service Federation for 5G & Beyond Public Working Group: Applications to Federated Autonomic/Autonomous Networking", in the IEEE Future Networks World Forum (FNWF), 13–15 November 2023 // Baltimore, MD, USA.

[49] I. Elgarhy, A. El-toukhy, M. Badr, M. Mahmoud, M. Fouda, M. Alsabaan, Hisham A. Kholidy, "Secured Cluster-Based Electricity Theft Detectors Against Blackbox Evasion Attacks", in the IEEE 21st Consumer Communications & Networking Conference (CCNC), 6-9 January 2024.

[50] M. C. Zouzou, E. Benkhelifa, Hisham A. Kholidy and D. W. Dyke, "Multi-Context-aware Trust Management framework in Social Internet of Things (MCTM-SIoT)," 2023 International Conference on Intelligent Computing, Communication, Networking and Services (ICCNS), Valencia, Spain, 19-22 June 2023, pp. 99-104, doi: 10.1109/ICCNS58795.2023.10193510.

[51] Hisham A. Kholidy, Andrew Karam, James Sidoran, et al. "Toward Zero Trust Security in 5G Open Architecture Network Slices", IEEE Military Conference (MILCOM), CA, USA, November 29, 2022. https://edas.info/web/milcom2022/program.html

[52] Hisham A. Kholidy, Andrew Karam, Jeffrey H. Reed, Yusuf Elazzazi, "An Experimental 5G Testbed for Secure Network Slicing Evaluation", the 2022 IEEE Future Networks World Forum (FNWF), Montreal, Canada, October 2022. https://fnwf.ieee.org/wp-content/uploads/sites/339/2022/10/AcceptedPaperScheduleV0.1.pdf

[53] Hisham A. Kholidy, Riaad Kamaludeen "An Innovative Hashgraph-based Federated Learning Approach for Multi Domain 5G Network Protection", the 2022 IEEE Future Networks World Forum (FNWF), Montreal, Canada, October 2022. https://fnwf.ieee.org/wp-content/uploads/sites/339/2022/10/AcceptedPaperScheduleV0.1.pdf

[54] Hisham A. Kholidy, Salim Hariri, "Toward an Experimental Federated 6G Testbed: A Federated leaning Approach", the 19th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA 2022), Abu Dhabi, UAE December 5th - December 7th, 2022

[55] Hisham Kholidy, Andrew Karam, James L. Sidoran, Mohammad A. Rahman, "5G Core Security in Edge Networks: A Vulnerability Assessment Approach", the 26th IEEE Symposium on Computers and Communications (The 26th IEEE ISCC), Athens, Greece, September 5-8, 2021. https://ieeexplore.ieee.org/document/9631531

[56] N. I. Haque, M. Ashiqur Rahman, D. Chen, Hisham Kholidy, "BIoTA: Control-Aware Attack Analytics for Building Internet of Things," 2021 18th Annual IEEE International Conference on Sensing, Communication, and Networking (IEEE SECON), 2021, pp. 1-9, doi: 10.1109/SECON52354.2021.9491621.

[57] Samar SH. Haytamy, Hisham A. Kholidy, Fatma A. Omara, "Integrated Cloud Services Dataset", Springer, Lecture Note in Computer Science, ISBN 978-3-319-94471-5, https://doi.org/10.1007/978-3-319-94472-2. 14th World Congress on Services, 18-30. Held as Part of the Services Conference Federation, SCF 2018, Seattle, WA, USA.

[58] Hisham A. Kholidy, Ali Tekeoglu, Stefano Lannucci, Shamik Sengupta, Qian Chen, Sherif Abdelwahed, John Hamilton, "Attacks Detection in SCADA Systems Using an Improved Non- Nested Generalized Exemplars Algorithm", the 12th IEEE International Conference on Computer Engineering and Systems (ICCES 2017), published in February 2018.

[59] Stefano Iannucci, Hisham A. Kholidy Amrita Dhakar Ghimire, Rui Jia, Sherif Abdelwahed, Ioana Banicescu, "A Comparison of Graph-Based Synthetic Data Generators for

Benchmarking Next-Generation Intrusion Detection Systems", IEEE Cluster, Sept 5 2017, Hawaii, USA.

[60] Qian Chen, Hisham A. Kholidy, Sherif Abdelwahed, John Hamilton, "Towards Realizing a Distributed Event and Intrusion Detection System", the International Conference on Future Network Systems and Security (FNSS 2017), Gainesville, Florida, USA, 31 August 2017.

[61] Hisham A. Kholidy, Abdelkarim Erradi, "A Cost-Aware Model for Risk Mitigation in Cloud Computing Systems", 12th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA), Marrakech, Morocco, November, 2015.

[62] Hisham A. Kholidy, Abdelkarim Erradi, Sherif Abdelwahed, "Attack Prediction Models for Cloud Intrusion Detection Systems", in the International Conference on Artificial Intelligence, Modelling and Simulation (AIMS2014), Madrid, Spain, November 2014.

[63] Hisham A. Kholidy, Ahmed M. Yousouf, Abdelkarim Erradi, Hisham A. Ali, Sherif Abdelwahed, "A Finite Context Intrusion Prediction Model for Cloud Systems with a Probabilistic Suffix Tree", in the 8th European Modelling Symposium on Mathematical Modelling and Computer Simulation, Pisa, Italy, October 2014.

[64] Hisham A. Kholidy, A. Erradi, S. Abdelwahed, "Online Risk Assessment and Prediction Models For Autonomic Cloud Intrusion Prevention Systems", in the "11th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA), Doha, Qatar, November 2014.

[65] Hisham A. Kholidy, Abdelkarim Erradi, Sherif Abdelwahed, Abdulrahman Azab, "A Finite State Hidden Markov Model for Predicting Multistage Attacks in Cloud Systems", in the 12th IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC), Dalian, China, August 2014.

[66] Hisham A. Kholidy, Abdelkarim Erradi, Sherif Abdelwahed, Fabrizio Baiardi, "A Hierarchical, Autonomous, and Forecasting Cloud IDS", the 5th Int. Conference on Modeling, Identification and Control (ICMIC2013), Cairo, Aug31-Sept 1-2, 2013.

[67] Hisham A. Kholidy, Abdelkarim Erradi, Sherif Abdelwahed, Fabrizio Baiardi, "HA- CIDS: A Hierarchical and Autonomous IDS for Cloud Environments", Fifth International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN) Madrid, Spain, June 2013.

[68] Hisham A. Kholidy, Fabrizio Baiardi, "CIDD: A Cloud Intrusion Detection Dataset for Cloud Computing and Masquerade Attacks", the 9th International Conference on Information Technology: New Generations (ITNG), Las Vegas, Nevada, USA, 2012.

[69] Hisham A. Kholidy, Fabrizio Baiardi, "CIDS: A framework for Intrusion Detection in Cloud Systems", The 9th International Conf. on Information Technology: New Generations (ITNG), Las Vegas, Nevada, USA, 2012.

[70] Hisham A. Kholidy, Chatterjee N., "Towards Developing an Arabic Word Alignment Annotation Tool with Some Arabic Alignment Guidelines", the 2010 10th International Conference on Intelligent Systems Design and Applications (ISDA), pp 778-783, Cairo, Egypt, vol. IEEE Catalog Number: CFP10394-CDR, 2010.

[71] Hisham A. Kholidy, Khaled S. Algathber, "A New Accelerated RC4 Scheme using "Ultra Gridsec" and "HIMAN", 5th Int. Conference on Information Assurance and Security, Aug 2009, China.

[72] Hisham A Kholidy, A. Azab, S. Deif, "Enhanced ULTRA GRIDSEC: Enhancing High- Performance Symmetric Key Cryptography Schema Using Pure Peer-to-Peer Computational Grid Middleware (HIMAN)", IEEE-ICPCA (the 3rd Int. Conf. on Pervasive Computing and Applications, 06-08 Oct 2008.

[73] A. Azab, Hisham A Kholidy, "An Adaptive Decentralized Scheduling Mechanism for Peer-to-Peer Desktop Grids", International Conference on Computer Engineering & Systems Nov 2008.

[74] Mostafa-Sami M., Safia H D., Hisham A Kholidy, "ULTRAGRIDSEC: Peer-to-Peer Computational Grid Middleware Security Using High-Performance Symmetric Key Cryptography" in IEEE-ITNG (5th Int. Conf. On Information Technology-New Generations), LasVegas, Nevada, USA, 7-9 April 2008.

[75] Mohammed Arshad, Patel Tirth, Hisham Kholidy, "Deception Technology: A Method to Reduce the Attack Exposure Time of a SCADA System", https://dspace.sunyconnect.suny.edu/handle/1951/70148,

[76] Akshay Bhoite, Diwash Basnet, Hisham Kholidy, "Risk Evaluation for Campus Area Network", https://dspace.sunyconnect.suny.edu/handle/1951/70162

[77] Malkoc, M., & Kholidy, H. A. (2023). 5G Network Slicing: Analysis of Multiple Machine Learning Classifiers. ArXiv. /abs/2310.01747.

[78] Fathy M. Mustafa, Hisham A. Kholidy, Ahmed F. Sayed et al. Distributed Backward Pumped Raman Amplifier Gain Enhancement: New Approaches, 06 April 2023, available at Research Square [https://doi.org/10.21203/rs.3.rs-2770728/v1]

[79] Grippo, T., & Kholidy, H. A. (2022). Detecting Forged Kerberos Tickets in an Active Directory Environment. arXiv. https://doi.org/10.48550/arXiv.2301.00044

[80] Zielinski, D., & Kholidy, H. A. (2022). An Analysis of Honeypots and their Impact as a Cyber Deception Tactic. arXiv. https://doi.org/10.48550/arXiv.2301.00045

[81] Kholidy, H. A., & Abuzamak, M. (2022). 5G Network Management, Orchestration, and Architecture: A Practical Study of the MonB5G project. arXiv. https://doi.org/10.48550/arXiv.2212.13747

[82] Abuzamak, M., & Kholidy, H. (2022). UAV Based 5G Network: A Practical Survey Study. arXiv. https://doi.org/10.48550/arXiv.2212.13329

[83] Kholidy, H. A., Rahman, M. A., Karam, A., & Akhtar, Z. (2022). Secure Spectrum and Resource Sharing for 5G Networks using a Blockchain-based Decentralized Trusted Computing Platform. arXiv. https://doi.org/10.48550/arXiv.2201.00484

[84] Kholidy, H. A. (2021). State Compression and Quantitative Assessment Model for Assessing Security Risks in the Oil and Gas Transmission Systems. arXiv. https://doi.org/10.48550/arXiv.2112.14137

[85] Kholidy, H. A. (2021). A Triangular Fuzzy based Multicriteria Decision Making Approach for Assessing Security Risks in 5G Networks. arXiv. https://doi.org/10.48550/arXiv.2112.13072

[86] Haque, N. I., Rahman, M. A., Chen, D., & Kholidy, H. (2021). BIoTA Control-Aware Attack Analytics for Building Internet of Things. arXiv. https://doi.org/10.48550/arXiv.2107.14136

[87] Kholidy, H. A. (2020). Cloud-SCADA Penetrate: Practical Implementation for Hacking Cloud Computing and Critical SCADA Systems. Department of Computer and Network Security, College of Engineering, SUNY Polytechnic Institute. http://hdl.handle.net/20.500.12648/1605

[88] Hisham A. Kholidy, Abdelkader Berrouachedi, Elhadj Benkhelifa and Rakia Jaziri, "Enhancing Security in 5G Networks: A Hybrid Machine Learning Approach for Attack Classification", the 10th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA), December 4-7, Cairo, Egypt.

[89] Soufiane Hamadache, Elhadj Benkhelifa, Hisham kholidy,Pradeeban Kathiravelu, Brij B Gupta, "Leveraging SDN for Real World Windfarm Process Automation Architectures", The 10th International Conference on Software Defined Systems (SDS-2023) San Antonio, Texas , USA. October 23-25.

[90] Adda Boulem, Abdelkader Berrouachedi, Marwane Ayaida, Hisham Kholidy and Elhadj Benkhelifa, "A New Hybrid Cipher based on Prime Numbers Generation Complexity: Application in Securing 5G Networks", the IEEE Federated Architectures & Testbeds Workshop on 5G and Beyond (FATW5G 2023), December 6-7, Smart Village Giza, Egypt.

[91] Meriem Chiraz zouzou, mohamed shahawy, Elhadj Benkhelifa and Hisham Kholidy, "SIoTSim: Simulator for Social Internet of Things", The 10th International Conference on Internet of Things: Systems, Management and Security (IOTSMS 2023). San Antonio, Texas, USA. October, 2023.

[92] Hisham A. Kholidy, Keven Disen, Andrew Karam, Elhadj Benkhelifa, Mohammad A. Rahman, Atta-Ur Rahman, Ibrahim Almazyad, Ahmed F. Sayed and Rakia Jaziri, "Secure the 5G and Beyond Networks with Zero Trust and Access Control Systems for Cloud Native Architectures", the IEEE Federated Architectures & Testbeds Workshop on 5G and Beyond (FATW5G 2023), December 6-7, Smart Village Giza, Egypt.

[93] Ibrahim Almazyad, Sicong Shao, Salim Hariri and Hisham Kholidy, "Anomaly Behavior Analysis of Smart Water Treatment Facility Service: Design, Analysis and Evaluation", the 10th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA), December 4-7, Cairo, Egypt.

[94] Abdulbast A Abushgra, Hisham A Kholidy, Abdelkader Berrouachedi and Rakia Jaziri, "Innovative Routing Solutions: Centralized Hypercube Routing Among Multiple Clusters in 5G Networks", the IEEE Federated Architectures & Testbeds Workshop on 5G and Beyond (FATW5G 2023), December 6-7, Smart Village Giza, Egypt.

[95] Adda Boulem, Cyril De Runz, Hisham Kholidy, Abdelmalek Bengheni, Djahida Taib, Marwane Ayaida, "A New Classification of Target Coverage Models in WSNs, Survey and Algorithms and Future Directions", The 7th International Conference on Information and Computer Technologies (ICICT 2024), March 15-17, Honolulu, Hawaii.