UMYU Scientifica, Vol. 2 NO. 4, December 2023, Pp 201 – 211
https://doi.org/10.56919/usci.2324.025
ISSN: 2955 – 1145 (print); 2955 – 1153 (online)
A periodical of the Faculty of Natural and Applied Sciences, UMYU, Katsina

REVIEW ARTICLE

Enhancing Security of 5G-Enabled IoT Systems through Advanced Authentication Mechanisms: A Multifaceted Approach

Umar Danjuma Maiwada, Kamaluddeen Usman Danyaro, Aftab Alam Janisar, Mujaheed Abdullahi.
Department of Computer and Information Science, Universitit Teknologi PETRONAS, Malaysia.

ABSTRACT

The Internet of Things (IoT) has revolutionized device communications, offering unprecedented efficiency and convenience. However, the widespread adoption of IoT has raised significant security concerns, emphasizing the need for robust security measures. This study focuses on the crucial aspect of authentication within the layered architecture of IoT systems. Authentication is foundational to the architecture, ensuringIoT services and datae availability, security, and integrita. The research evaluates the current state of IoT authentication techniques, highlighting limitations in conventional solutions.Ann advanced authentication framework is propose to address these shortcomingsd, incorporating cutting-edge technologies such as blockchain, artificial intelligence, and biometrics. The framework employs biometric data for a dynamic and adaptive authentication process, enhancing security and accuracy in user and device identification. Blockchain technology is integrated to establish a decentralized and tamper-resistant identity management system, reducing the risk of unauthorized access and data manipulation. Artificial intelligence continuously adapts authentication processes based on behavioural patterns, bolstering the system's resilience against evolving cyber threats. The study also discusses the practical application of the proposed authentication system, considering resource limitations in IoT devices. It provides insights into thesuggested solution's efficiency, scalability, and interoperability within various IoT ecosystems. The research contributes to the ongoing discourse on IoT security by thoroughly examining enhanced authentication procedures. Organizations can fortify their IoT deployments against a growing array of cyber threats by prioritizing advanced authentication within a layered design, fostering a more secure and reliable IoT ecosystem. Additionally, the study presents a comprehensive overview of the state-of-the-art security in IoT, exploring various designs, enabling technologies, and protocols. It delves into security challenges at each architectural tier, providing an in-depth analysis of attack taxonomies and advanced defenses. The article serves as a valuable resource for researchers and academics in the IoT sector, offering a detailed survey of architectural security, identification of challenges, resolution strategies, and insights into the evolving landscape of IoT. The study provides a comprehensive survey of IoT architectural security, identifying challenges, proposing resolutions, and highlighting changes in the IoT domain. This research aims to enhance the accuracy by 80% of IoT security, fostering a more secure and reliable IoT ecosystem.

ARTICLE HISTORY

Received August 01, 2023.
Accepted November 29, 2023.
Published December 30, 2023.

KEYWORDS

Behavioural, Internet of things IOT, cyber threats, DDoS, Authentication, IDS

INTRODUCTION

A new era of connectivity has arrived with the introduction offifth-generationn (5G) wireless technology, which promises unheard-of speed, minimal latency, and widespread device connectivity. Strong security measures are more important than ever as 5G networks take on a central role on the Internet of Things (IoT), allowing a vast array of connected devices to communicate with each other seamlessly.The article discusses the necessity of doing so too strengthen the security of 5G-enabled IoT systemo. Specifically, it emphasizes how to improve authentication procedures inside a layered architecture that might improve security (Ahmad et al., 2019). IoT and 5G integration have the potential to revolutionize many sectors and enable smart cities, driverless cars, and a host of other cutting-edge uses. But increased connectivity and data sharing also mean a higher danger of cyberattacks. Authentication methods and other conventional security procedures might not be

Correspondence: Umar Danjuma Maiwada. Department of Computer and Information Science, Universitit Teknologi PETRONAS. ✉ Umar.danjuma@umyu.edu.ng.

How to cite: Danjuma, U. M., Usman, K. D., Alan, A. J., & Abdullahi, M. (2023). Enhancing Security of 5G-Enabled IoT Systems through Advanced Authentication Mechanisms: A Multifaceted Approach. *UMYU Scientifica*, 2(4), 201 – 211. https://doi.org/10.56919/usci.2324.025

enough to protect the dynamic and varied world of 5G-enabled IoT devices.This studyfocuses on the crucial function of authentication in the tiered architecture of IoT ecosystems powered by 5G. As the key to guaranteeingdatae privacy, availability, and integrita, authentication needs to be improved and reevaluated to meet the ever-changing threats from highly skilled cybercriminals (Ahmad & Alsmadi, 2021). We examine the current authentication techniques used in 5G IoT networks, examining their shortcomings and vulnerabilities to new attacks. Also, by acknowledging the necessity of a proactive and flexible security strategy, we put forth an intricate authentication framework that fortifies the layers of 5G IoT architecture by utilizing cutting-edge technology. The suggested framework creates a multi-layered defence against unwanted access and data breaches by incorporating cutting-edge authentication technologies like biometrics, blockchain, and artificial intelligence. Our method integrates these technologies to create a scalable, robust, and dynamic authentication process that is specific to the demands of 5G-enabled Internet of Things environments. By promoting a thorough and flexible authentication approach, we hope to further the conversation around 5G security on the Internet of Things. Using sophisticated authentication techniques is essential as the linked world develops to preserve data integrity, respect user privacy, and guarantee the continuous operation of 5G-enabled IoT devices (Ali et al., 2015).

The enhancement of 5G security within the Internet of Things (IoT) layered architecture through advanced authentication mechanisms is a critical aspect of ensuring the integrity, confidentiality, and reliability of IoT systems. This paper focuses on addressing security challenges in the context of 5G-enabled IoT networks, with a specific emphasis on authentication procedures. The content of the paper has been structured as follows: Introduction, Background, Current State of 5G Security in IoT, Advanced Authentication Mechanisms, Proposed Enhanced Authentication Framework, Implementation and Practical Considerations, Conclusion. By addressing these key points, the paper aims to provide a comprehensive understanding of how advanced authentication mechanisms can enhance 5G security within the layered architecture of IoT systems. The aim of the research is to improve the security of 5G-enabled Internet of Things (IoT) systems by implementing advanced authentication mechanisms within the layered architecture. The goal is to address the unique security challenges posed by the integration of 5G technology into IoT ecosystems and provide a robust framework that ensures the confidentiality, integrity, and reliability of data exchanged among connected devices. The objectives are as follows: Evaluate the existing security posture of IoT systems in the context of 5G technology. Identify vulnerabilities, threats, and potential risks introduced by the integration of 5G. Develop a comprehensive authentication framework tailored specifically for 5G-connected IoT devices. Ensure the framework addresses the unique challenges posed by the layered architecture of IoT systems. Offer practical recommendations for the integration of advanced authentication mechanisms in 5G-enabled IoT deployments. Consider implications for industry standards and best practices.

This research will explore the elements of our suggested authentication system in more detail as well as its potential applications and implications for the security environment of 5G-driven IoT in the following sections. In today's world, the Internet of Things (IoT) is a sophisticated and promising technology. This is a relatively new and developing technology that is becoming more and more well-known every day. With the use of smart items, communication, and actuation capabilities, the Internet of Things (IoT) connects real and virtual objects, things, and devices in a unique way. Anything and everything can be effortlessly and constantly connected to anything and everything, anytime, anyplace, according to the Internet of Things concept. Radio Frequency Identification (RFID) was the first technology used to connect items; barcode, wired, and wireless connectivity followed later (Sarker et al., 2023). The concept of the Internet of Things (IoT) turns a computer set into a collection of connected things. There are more objects in our environment than there are people who own them, including machinery, goods, transportation, and residential appliances. As of right present, the Internet of Things lacks defined standards and structures. IoT is referred regarded by some as a new paradigm that incorporates wireless communications technology including actuators, mobile networks, and wireless sensor networks. Every IoT component has a name and ought to have a distinct address. IoT devices initially use RFID for communication. IoT is expected to connect every aspect of our life by 2025, according to the US National Intelligence Council (USNIC). Over the past ten years, the goal has suggested alternative architectures and created new research problems (Said & Masud, 2013). The Internet of Things has surpassed all previous technologies in our daily lives. It has completely changed how individuals communicate and operate in society. The MIT AutoID Centre is credited with officially coining the term "IoT" in 2001 (Benabdessalem et al., 2014). Through the integration of billions of things, the Internet of Things (IoT) enhances communications and computation. Smart objects that can understand and communicate with each other can be created from common place objects through the use of detectors, RFID, internet connectivity, and localization technologies (Amaral et al., 2011).

The embedded sensors in smart objects have the ability to perceive, record, and monitor a wide range of data about the environment, human social interaction, and equipment (Khanam et al., 2020). IOT is a collection of interconnected technologies that work together to deliver seamless services; it is not just one technology. The security and other features that IOT devices received are largely dependent on the framework on which it is built. As anticipated in, there were currently more connected gadgets than individuals (Gubbi et al., 2013) According to Cisco, there will be seven times as many networked devices on the planet in 2020 as people, or 50 billion, and these gadgets will continuously add gigabytes of data (Piyare, 2013). Technologies like UMTS, WiFi, CSM, Bluetooth, ZigBee, and WiFi might link those millions of devices together (Khattak et al., 2019). The Internet of Things has surpassed all previous technologies in our daily lives. It has completely changed how people think and communicate. With an expected 24.6 billion IOT connections by 2025 and a 13 percent yearly compound growth in CAICT, the IOT size is expanding quickly (Aghili et al., 2021). As per the strategic analytics (Datta, 2022), more than 38 billion interconnected items will exist by the end of 2025, and by 2030, there will be 50 billion connected objects. Within the work of (Fan et al., 2021), According to International Data Corporation (IDC), 41 billion gadgets will be connected by 2025, generating roughly 79 terabytes of data. According to another study, there are already 50 billion device connections, and by 2025, there will be 75.44 billion (Kumar et al., 2022). Numerous facets of our lives have changed significantly because of IoT technology. Additionally, it has become an essential facilitator of creativity and achievement in a variety of sectors, such as transportation, machine-to-machine (M2M), vehicle-to-vehicle (V2V), and IoT-based smart environments (Karie et al., 2020), and numerous others. 2021 IoT-Based Smart Environment Security Frameworks and Standards with the use of laptops, smartphones, and tablets, users of smart technologies can connect to and operate smart appliances and equipment remotely over the internet (Kebande et al., 2018).

IoT nodes are made to be able to configure themselves, including self-configuration, maintaining themselves, self-repair, self-connection, self-identification, and the ability to make decisions on their own, when they are placed in new environments. As IoT advances, issues establishing a smart environment with sustainable applications will arise. Scalable storage and IoT-compliant architectures are necessities. Modern IoT consists of a set of diverse technologies used to develop applications across multiple industries. IoT technologies allow apps to become smart by evaluating data from sensors and recognizing parameters of the real world. IoT has numerous security-sensitive issues despite its usefulness. Connections between people, things, sensors, and services are ubiquitous and ongoing. The security system is still dependent on human interaction, which makes it vulnerable to security threats despite any clever configuration, effective implementation, and careful maintenance. Therefore, while designing cybersecurity solutions, human input is required (Stout & Urias, 2016). IoT is valuable, however there are a lot of sensitive security issues. Connections between people, things, sensors, and services are constant and universal. Even with excellent design, meticulous configuration, effective implementation, and upkeep, human intervention will still be vulnerable to security risks. Thus, human considerations are necessary in the planning of cybersecurity solutions (Karie et al., 2021). IoT must get past significant obstacles before it can be trusted by the public, but it has already shown that it can significantly expand the applications in logistics, transportation, and health. As a result, IoT is seen as a component of the internet of the future, where anything can connect and communicate with one another. IoT limitations include things like size, power usage, processing power, and storage capacity. Network-based restrictions include scalability, mobility, and slow, sporadic network connections that result in low power rates since low power radio implementation is used. Software-based restrictions include embedded software limitations. Therefore, privacy in IoT is right now the largest issue and needs researchers' attention (Alsharif et al., 2023). However, because of the scale or number of sites in the system as well as the diversification of devices and protocols, implementing security methods in an Internet of Things system is more difficult than in a typical network. The difficulties in implementing IoT security measures because of physical pairing, heterogeneity, resource limitations, enormous magnitude, trust management, and inadequate security planning. However, systems and equipment that are linked to the Internet are subject to a variety of security concerns and threats in addition to the data it can sense, gather, and communicate. Furthermore, as every connected device has the potential to be a point of entry or attack for malevolent actors, it is imperative to assess and fortify the protection of IoT-based intelligent settings. We must prioritize data availability, access control, encryption, and authentication when it comes to securing IOT networks. There is a constant need for security measures to be established to overcome emerging security difficulties, even though numerous research efforts have presented numerous answers to the threats in IoT, which has greatly helped the IoT security problem mitigation. Finding a need for the study is the first stage in performing a literature review. In our instance, we completed this assignment by realizing that gaps and patterns in the IoT security components included in this study which is needed to be found.

Scalability refers to a system's capacity to handle an increasing amount of work as a result of an increase in components while maintaining system functionality (Ali et al., 2015). According to (Yu & Guo, 2019), In order to handle the exponential development of IoT technology and information generation, systems for scaling must be put into place. The authors also emphasized the need of IIoT scalability, highlighting the key concerns pertaining to heterogeneity of devices, network diversity, and the massive volumes of data produced by IIoT systems (Mirani et al., 2022). Cloud-based services and intricate physical device networks are components of Internet of Things (IoT) systems, which store and analyse vast volumes of data produced by devices. IoT applications should be able to communicate with the outside world in a way that is defined by cloud-based architectures, which also make data sharing with independent Web services easier (Rath et al., 2023). Because of device complexity and the sheer number of devices used in an IoT domain, scaling the architecture of an IoT is still difficult. IOT applications and scalability demand many devices. For instance, millions of devices might be needed to determine temperature fluctuations throughout a whole nation. This would result in massive volumes of data that would be challenging to handle, interpret, store, and deploy (Jing et al., 2014). Several kinds of actuators and sensors make up the majority of IoT systems. As a result, there are differences in data formats and protocols for communication, which makes IoT settings more complex and presents a significant obstacle when combining services and data with other business applications (Javed et al., 2020). After aggregation, the constituent service should also be readily upgradeable and reachable with a minimal response time. Once again, the service included in the design structure needs to be reusable because it speeds up the process of construction and upgrading and facilitates the integration of IoT systems with new technologies (Santana et al., 2021). Furthermore, it ought to facilitate the adaptability of switching between different computer environments (Lai et al., 2019). Finally, to guarantee that IoT applications operate appropriately, safely, and effectively, ongoing upgrading, integration, and maintenance are required (Cerny, 2019). For these to be developed, managed, and broken down into specialized services, a structure for Internet of Things applications is needed. In order to achieve this, data-driven interfaces and other microservices are used, and they are designed as autonomous, self-sufficient processes (Dragoni et al., 2017).

Technology that uses password encryption can safeguard information. The collection of keys from limitless channels, hash chain protocol, random hash lock protocol, encryption, and encrypted identifiers are only a few examples of the various encryption technologies. IoT faces two security issues: the first is inherent to the technology itself; as it integrates several heterogeneous networks, it must address compatibility-related security issues with those networks. The other one is about building and deploying IOT networks; factors like DoS assaults, WLAN application conflicts, IPV6 application risk, intermediate attacks, and heterogeneous network attacks all have an impact on IoT transport (Mirani et al., 2022). We discovered certain similar themes in the areas of developing technologies and difficulties on the Internet of Everything & IIOT architecture. To create end-to-end Internet of Things systems, layer architectures use developing technologies to address important requirements. We showcase the most recent findings on how layer designs, categorized by edge/wind computation, a blockchain, SDN, 5G, AI, machine learning, and wireless sensor network (WSN) technologies, meet these needs. To address IIoT applications' deficiency in predictive maintenance, the reference (Moens et al., 2020) suggests a cloud- and edge-based smart machine maintenance architecture for low latency, safety, and network scalability. With the aid of three IIRA models, the suggested system also satisfies the requirement for large amounts of data for suitable and trained algorithms. Using machine learning methods, a fleet of multi-noded machines transmits data to an edge device for data analytics and to convey diagnostic data to the platform level for user monitoring. Although it does not address the primary issues, the suggested architecture makes use of machine learning to anticipate maintenance needs. Cloud services cannot manage large-scale data processing because of the manufacturing industry's massive and diverse data creation. Moreover, delayed information is susceptible since cloud services are inherently semi-secure. Sengupta et al. suggested an industrial Internet of things architecture based on fog computing technologies in this area. Fog nodes, cloud layers, application layers, and perception layers form the foundation of the suggested approach. The author introduced a semi-secure cloud computing feature that includes fog nodes and virtual operating systems (OS), which can be PCs, Raspberry Pi devices, or nodes, to process data and lessen workload from cloud computing. The authors created a hardware test bed and conducted simulation studies, but the suggested approach ignored the compatibility of heterogeneous field equipment and reliability in the demanding industrial context (Ghosh et al., 2021).

From the research of [30], By developing fault tolerant IIoT architectures that use edge gateways and offer low latency, scalability, and safety according to industrial requirements, the authors overcome the weaknesses in system reliability. The author used a Raspberry Pi edge device to store data in a local database and created a system to determine the state of machine operation. To forecast the machine's condition and show monitoring metrics like current, power consumption, and vibration, edge devices employ these data in algorithms. By moving data closer to the edge, the suggested system in edge computing prevents data transfer delays and congestion, as well as increases data security. The research presented in (Ungurean & Gaitan, 2020) an architectural paradigm designed to solve interoperability issues and integrate the various field buses. The suggested paradigm moves information processing toward edge/fog nodes, ensuring data protection. High network scalability is further enhanced by the capacity to disperse edges and fog nodes across several domains. The four layers of the suggested model—the sensor layer, the knowledge provider layer, that foam/edge calculation layer, and the application/service layer—are also predicated on the communication process' dependability and low latency. Devices and peripherals linked to certain field buses, such Modbus and Ethernet, are included in the sensor layer. As the Fog/Edge Computation Layer processes the data, the Data Supplier layer saves the two-way data from the field bus and the higher layer in the buffered memory. Applications that are built for remote control and monitoring are provided via the application/service layer. Although the compatibility of M2M communications across network elements has been emphasized by the authors, data privacy issues are not addressed in the concept model. The future of manufacturing procedures lies in distributed automation systems, which use a variety of technologies, guidelines, and devices from various vendors. Nevertheless, because the current system has many connected devices, privacy and interoperability issues arise when information is exchanged efficiently. Dobaj et al. put forth a contemporary, lightweight, adaptable, and secure industrial Internet of things theoretical framework that incorporates perpetual system integration and growth (CI/CD) procedures within a containerized setting. With dispersed edge/fog nodes, network scalability and low latency are made possible.

Many existing studies have not specifically addressed the security challenges arising from the integration of 5G technology into IoT systems. The research finds a gap in the literature regarding dedicated exploration of security issues and solutions in this context. The layered architecture of IoT systems have not been extensively investigated concerning its specific impact on security in the 5G context. The research aims to fill this gap by exploring how the layered structure influences security requirements and solutions. The literature lacks comprehensive frameworks that integrate multiple advanced authentication mechanisms into a cohesive system designed for the specific challenges presented by 5G-connected IoT. The research aims to bridge this gap by proposing and evaluating a holistic authentication framework. The literature has not thoroughly explored how advanced authentication mechanisms interact and interoperate within the broader 5G ecosystem. The research has assessed interoperability challenges and propose solutions to ensure seamless integration.

METHODOLOGY

We conduct a comprehensive review of existing literature on 5G security and IoT authentication mechanisms. By defining specific authentication requirements considering the unique characteristics of 5G networks and the diverse IoT devices, we identify key security goals, including confidentiality, integrity, and availability. Then we understand the constraints and challenges imposed by the 5G IoT environment when analysing the current challenges, vulnerabilities, and shortcomings in authentication approaches within 5G-enabled IoT systems. Later we Identify state-of-the-art technologies and methods for enhancing authentication in layered architectures. As such, we define the specific authentication requirements pertinent to 5G-enabled IoT layered architecture. Hence, by considering factors such as device diversity, dynamic network conditions, and the need for low-latency authentication we determine the desired security goals, including confidentiality, integrity, and availability, within the context of IoT deployments on 5G networks. But, by developing a layered architecture that incorporates the selected authentication mechanisms seamlessly into the 5G-enabled IoT ecosystem, we designed the layers to accommodate the diverse range of IoT devices, ensuring scalability and efficiency while meeting the identified authentication requirements. We then try to implement a prototype or simulation of the proposed authentication framework to assess its feasibility and effectiveness. Later we utilize realistic scenarios and diverse IoT device profiles to evaluate the framework's performance, considering factors such as response time, accuracy, and resource consumption. We conduct a thorough security analysis of the developed prototype, evaluating its resilience against common cyber threats, including spoofing, replay attacks, and unauthorized access. The paper employ penetration testing and scenario-based simulations to identify potential vulnerabilities and refine the authentication mechanisms accordingly. An assessment for the scalability and compatibility of the proposed authentication framework with varying numbers and types of IoT devices was done. The paper considers the resource constraints of IoT devices and the ability of the framework to function seamlessly within the 5G network architecture. We evaluated the user experience of the enhanced authentication mechanisms by considering factors such as user acceptance, ease of use, and potential privacy concerns. We then gather feedback from users and stakeholders to refine the authentication processes for optimal usability. We validated the proposed methodology through peer review, expert consultation, and feedback from pilot implementations. Lastly, we iterate on the framework based on validation results and emerging security challenges in the rapidly evolving landscape of 5G-enabled IoT.

We assess the existing IoT layered architecture to identify potential security vulnerabilities in the 5G network. We then conduct a comprehensive risk assessment to understand the potential impact of security breaches on the 5G IoT architecture. We later implement advanced authentication mechanisms such as biometric authentication, multi-factor authentication, and certificate-based authentication to bolster security in the IoT layered architecture. We made another implementation of continuous monitoring tools and processes to detect and respond to security threats in real-time, enhancing the overall security posture of the IoT layered architecture. The 5G security in IoT layered architecture can be significantly enhanced through advanced authentication mechanisms. The software that was used for the analysis are NETSIM (NetSim Standard13.3.x64), Wireshark (V10), and MATLAB (2021).

To analyse the enhancement of 5G security in IoT layered architecture through advanced authentication mechanisms using NetSim (NetSim Standard13.3.x64), Wireshark, and MATLAB, these steps were followed: We simulate the 5G network with IoT devices using NetSim to replicate the layered architecture and authentication mechanisms. By utilizing NetSim to create a virtual environment for testing different authentication protocols and scenarios within the 5G network, we capture network traffic within the simulated 5G IoT architecture using Wireshark to analyse data packets and communication flows. The use of Wireshark to inspect the effectiveness of advanced authentication mechanisms by examining the encrypted data and authentication exchanges following the process of captured network data from Wireshark in MATLAB to perform in-depth analysis and visualization of authentication processes and encryption protocols. The utilization of MATLAB for statistical analysis of authentication success rates, encryption strength, and overall security performance within the 5G IoT architecture to integrate the data collected from NetSim and Wireshark into MATLAB for comprehensive analysis, allowing for a holistic assessment of the 5G security enhancements in the IoT layered architecture. By integrating NetSim for simulation, Wireshark for network traffic analysis, and MATLAB for advanced data processing and analysis, a thorough evaluation of the enhanced 5G security in IoT layered architecture through advanced authentication mechanisms was achieved.

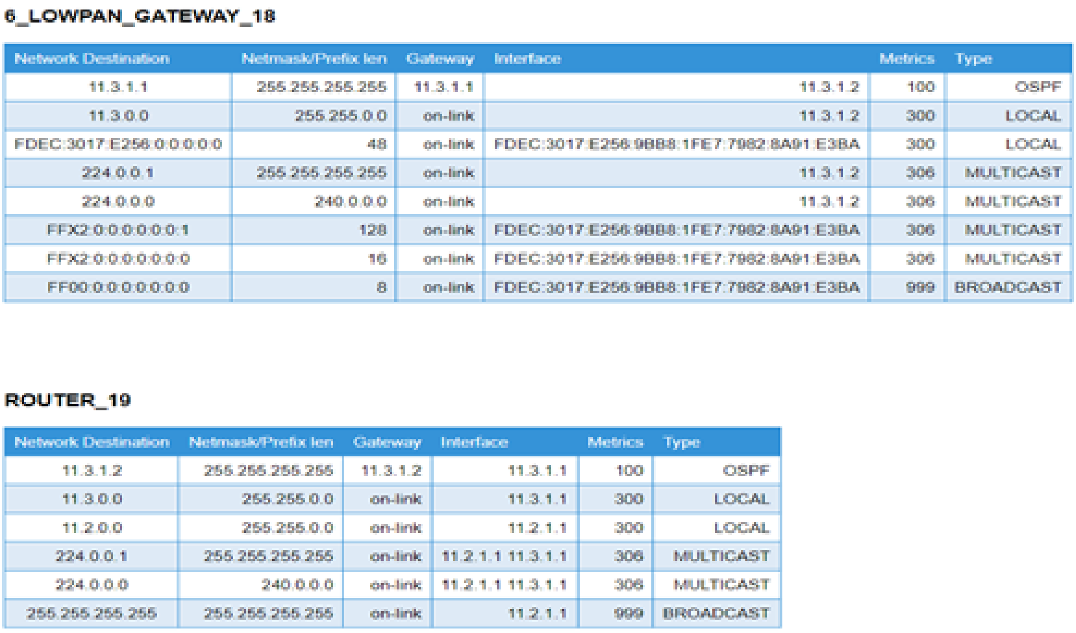
Table 1: Description of some attacks across IOT layers

Layers	Attacks	Description	Counter measure
PERCEPTION LAYER	Node capture attack	Replace or tamper with nodes or devices in the IoT	Monitor and detect malicious nodes
	Malicious virus attack	Attacks system by disguising itself as a self-propagating virus	Deploy a reliable firewall
	Replay attack	Attacker intercepts the sent message and replays it to sender or receiver	Deploy a strong authentication in place
	Dos / DDoS attack	Bombs network with very large traffic, occupying available resources	Increase network protection system
	Side channel attack	Leaked information is used to launch attack to physical systems	Authentication and strong cryptography
NETWORK LAYER	Routing information attack	Controlling the spread of information by manipulating routing protocols	Deploy a secure routing protocol
	Sinkhole attack	Infected device or node as a circular forwarding node	Add multiple security protocols
	Man-in-the-middle attack	Maliciously steal and control communication information between two normal devices	Deploying a secure communication protocol
	Wormhole attack	Send malicious packets through two malicious nodes or devices	Modify routing protocol
	Eavesdropping attack	Theft of data transmitted over a wireless link	Set secret key to filter noise data
APPLICATION LAYER	Code injection attack	Injecting malicious code into a node or device in the IoT	Verify the identity of the IoT code
	Phishing attack	Pretend to be a phishing website to trick user information	Be alert when users go online
	User impersonation attack	Attacker masks to access and claim all rights in the network	Authentication and continuous authentication

RESULT AND DISCUSSION

The paper utilizes MFA to bolster traditional username/password authentication, requiring additional verification such as biometrics, tokens, or one-time passcodes. Then later it employs digital certificates to authenticate IoT devices, ensuring secure and trusted communication within the 5G network. By implementing robust encryption protocols, such as Transport Layer Security (TLS) or Datagram Transport Layer Security (DTLS), to safeguard data transmission and prevent unauthorized access, we employ IAM solutions to manage and control access to IoT devices, enabling granular permissions and centralized authentication management. As seen in Figure 1 below, the implementation of a zero-trust security approach, which assumes no implicit trust, and continuously verifies device identity and authorization before granting access was required. Hence, the performance of frequent security assessments and audits to identify vulnerabilities, ensure compliance with security standards, and address any potential weaknesses in the authentication mechanisms was done by embracing the measures in 5G security IoT layered architecture which can be substantially strengthened, offering enhanced protection against various security threats from Figure 2.

Intelligent technology, intelligent mobility, intelligent governance, intelligent infrastructure, and intelligent health care are examples of IoT applications. Architectural design will consider each of these applications. Basic



6_LOWPAN_GATEWAY_18

Network Destination	Netmask/Prefix len	Gateway	Interface	Metrics	Type
11.3.1.1	255.255.255.255	11.3.1.1	11.3.1.2	100	OSPF
11.3.0.0	255.255.0.0	on-link	11.3.1.2	300	LOCAL
FDEC:3017:E256:0:0:0:0:0	48	on-link	FDEC:3017:E256:9BB8:1FE7:7982:8A91:E3BA	300	LOCAL
224.0.0.1	255.255.255.255	on-link	11.3.1.2	306	MULTICAST
224.0.0.0	240.0.0.0	on-link	11.3.1.2	306	MULTICAST
FFX2:0:0:0:0:0:0:1	128	on-link	FDEC:3017:E256:9BB8:1FE7:7982:8A91:E3BA	306	MULTICAST
FFX2:0:0:0:0:0:0:0	16	on-link	FDEC:3017:E256:9BB8:1FE7:7982:8A91:E3BA	306	MULTICAST
FF00:0:0:0:0:0:0:0	8	on-link	FDEC:3017:E256:9BB8:1FE7:7982:8A91:E3BA	999	BROADCAST

ROUTER_19

Network Destination	Netmask/Prefix len	Gateway	Interface	Metrics	Type
11.3.1.2	255.255.255.255	11.3.1.2	11.3.1.1	100	OSPF
11.3.0.0	255.255.0.0	on-link	11.3.1.1	300	LOCAL
11.2.0.0	255.255.0.0	on-link	11.2.1.1	300	LOCAL
224.0.0.1	255.255.255.255	on-link	11.2.1.1 11.3.1.1	306	MULTICAST
224.0.0.0	240.0.0.0	on-link	11.2.1.1 11.3.1.1	306	MULTICAST
255.255.255.255	255.255.255.255	on-link	11.2.1.1	999	BROADCAST

Figure 1: layer management

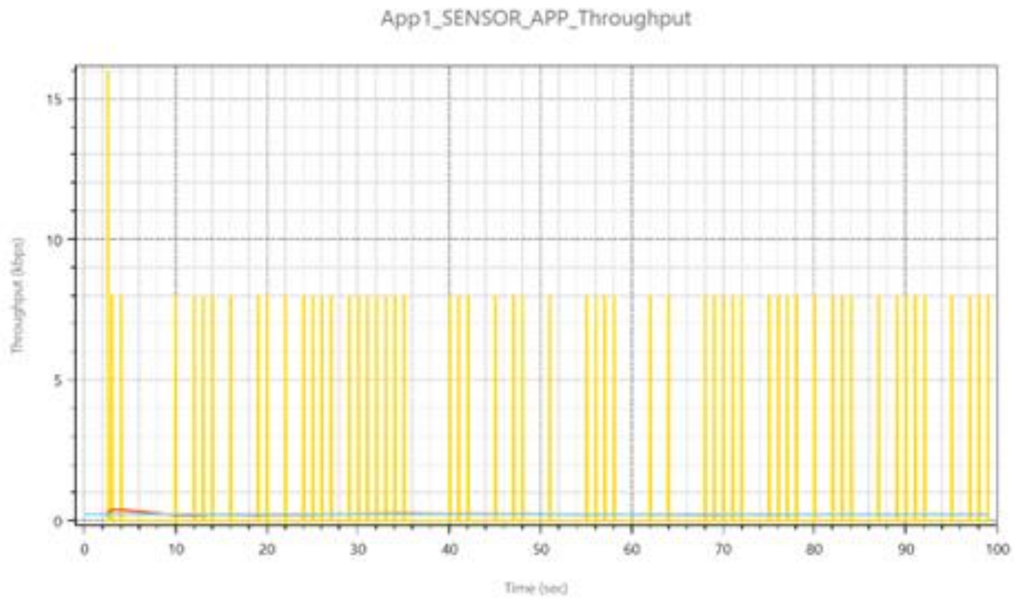
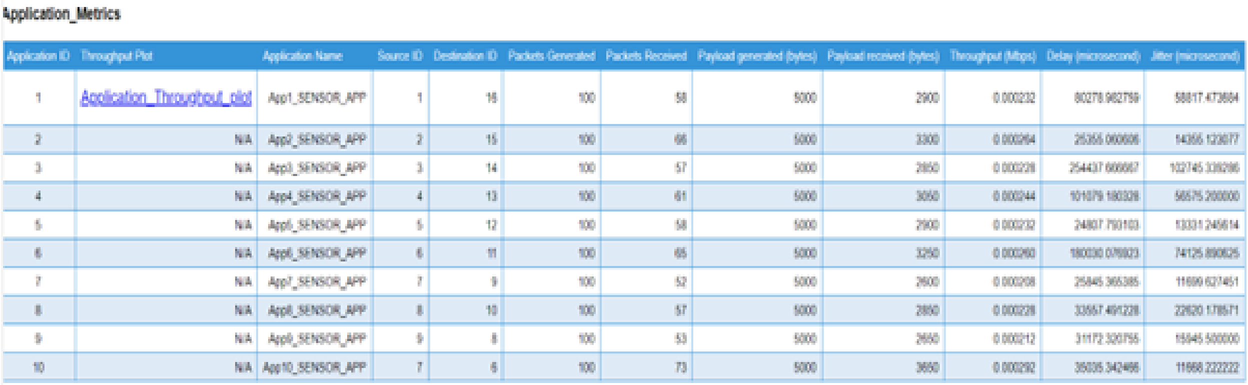


Figure 2: security threat



Application_Metrics

Application ID	Throughput Plot	Application Name	Source ID	Destination ID	Packets Generated	Packets Received	Payload generated (bytes)	Payload received (bytes)	Throughput (Mbps)	Delay (microsecond)	Jitter (microsecond)
1	Application_Throughput_plot	App1_SENSOR_APP	1	16	100	58	5000	2900	0.000232	80278.982759	58817.473684
2	N/A	App2_SENSOR_APP	2	15	100	66	5000	3300	0.000264	25355.060606	14355.123077
3	N/A	App3_SENSOR_APP	3	14	100	57	5000	2850	0.000228	254437.666667	102745.339286
4	N/A	App4_SENSOR_APP	4	13	100	61	5000	3050	0.000244	101079.180328	56575.200000
5	N/A	App5_SENSOR_APP	5	12	100	58	5000	2900	0.000232	24807.793103	13331.245614
6	N/A	App6_SENSOR_APP	6	11	100	65	5000	3250	0.000260	180030.076923	74125.890625
7	N/A	App7_SENSOR_APP	7	9	100	52	5000	2600	0.000208	25845.365385	11699.627451
8	N/A	App8_SENSOR_APP	8	10	100	57	5000	2850	0.000228	33557.491228	22620.178571
9	N/A	App9_SENSOR_APP	9	8	100	53	5000	2650	0.000212	31172.320755	15945.500000
10	N/A	App10_SENSOR_APP	7	6	100	73	5000	3650	0.000292	35035.342466	11668.222222

Figure 3: basic elements, application matrics

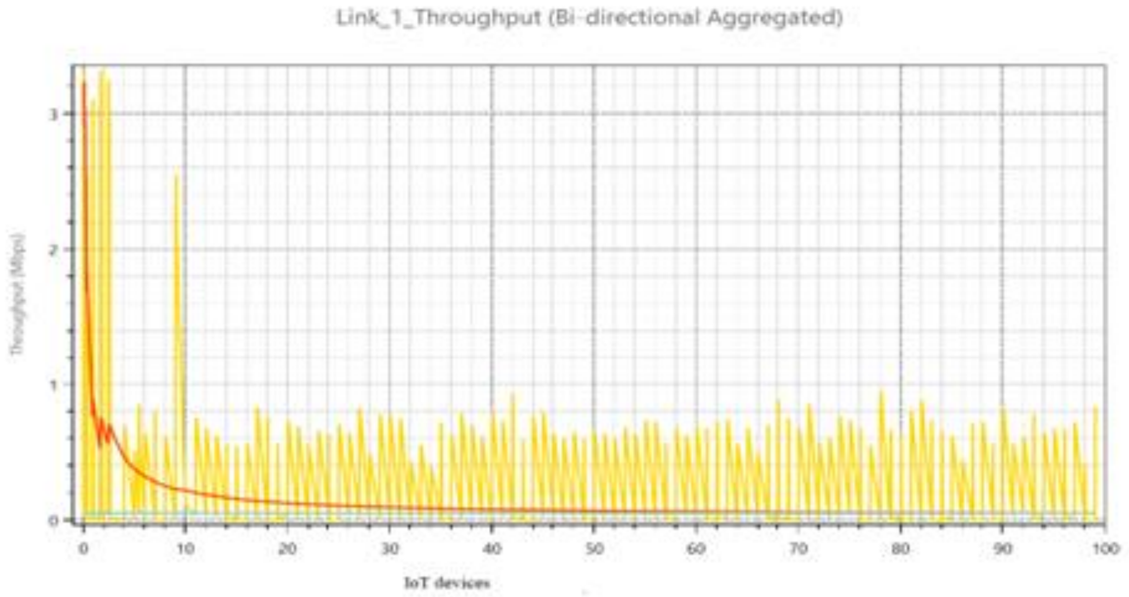
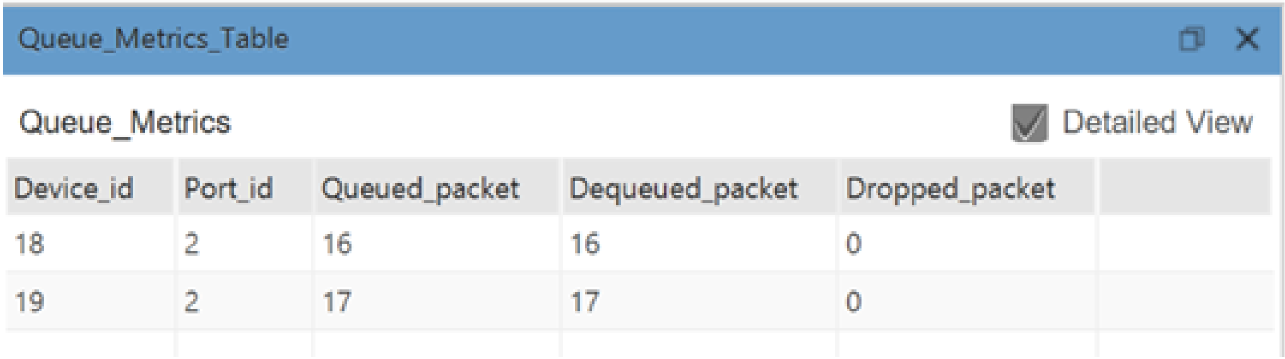


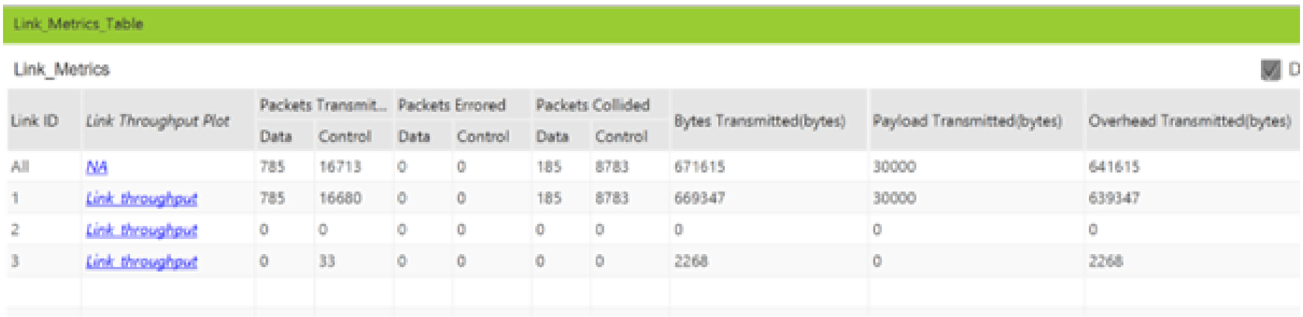
Figure 4: Performance of throughput Vs IoT devices


Queue_Metrics_Table

Queue_Metrics ☑ Detailed View

Device_id	Port_id	Queued_packet	Dequeued_packet	Dropped_packet
18	2	16	16	0
19	2	17	17	0

Figure 5: Queue matrics table for packets


Link_Metrics_Table

Link_Metrics ☑ D

Link ID	Link Throughput Plot	Packets Transmit...		Packets Errored		Packets Collided		Bytes Transmitted(bytes)	Payload Transmitted(bytes)	Overhead Transmitted(bytes)
		Data	Control	Data	Control	Data	Control			
All	NA	785	16713	0	0	185	8783	671615	30000	641615
1	Link throughput	785	16680	0	0	185	8783	669347	30000	639347
2	Link throughput	0	0	0	0	0	0	0	0	0
3	Link throughput	0	33	0	0	0	0	2268	0	2268

Figure 6: Link matrics that connects throughput and IoT devices.

elements including service quality (QoS), integrity, dependability, and integrity are addressed by IoT architecture as seen in Figure 3.

The authentication system needs to guarantee the following to guarantee the privacy of the IOT network as seen in Figure 4 above: User anonymity: To guarantee security, the system needs to preserve user anonymity. The attacker is unable to identify the user in real life. Unlikability: To increase privacy, the plan needs to stop hackers from keeping an eye on the user's activities. Mutual authentication: For users to validate one another, the system needs to offer mutual authentication. Agreements regarding session keys: the session key that is used for the encryption and decryption of the transmitted data needs to be unique and private. Resilience to various attacks: The system needs to accomplish all significant security goals and fend off any known attack. To overcome security flaws in specific user credentials, such as pins, passwords, and tokens that could be lost or stolen, biometrics offers distinctive identifying techniques. For a variety of causes, including dry or damaged skin or pollen on the printing sensor, the biometric properties of each input vary slightly. Certain writers have developed a code called "bio-hash," which uses user-specific pseudo-random token numbers to transfer physiological functions to binary strings.

Performance analysis shows the throughput, packet delivery ratio, and end-to-end delay. The protocol reduces communication costs and time in Figure 4. One bidirectional authentication method that prevents hackers from accessing wireless situations when transmitted data is at risk is two-factor authentication. In the design, we considered security criteria such mutual authentication, availability, privacy, governance, anonymity, and forwarding secrets. Afterwards, the threat model is designed to withstand denial-of-service (DoS), malevolent attacks, impersonation of users, online password guessing, replay, smart card theft, man-in-the-middle, inside, server counterfeit, parallel session see Figure 5 and Figure 6. Pre-calculation, registration, login, authentication, password change, and smart card withdrawal are the six stages of the suggested system. Following testing, the program gains resistance against attacks such as replay, password guessing, session key disclosure, and falsification. It also maintains user privacy, mutual authentication, key freshness, perfect forward secrets, freely selectable passwords, and no verification table. Traffic management, automated parking networks, remote monitoring of patients, inventory management, supply chain, consumption of energy control, supermarket personalization, and civil protection are just a few of the industries that can benefit from IoT's numerous uses. Other applications require the protection of their data and sensitive personal information about their whereabouts, routines, and social interactions, including credit card details and other financial data to put their privacy needs respectively.

Implementation of advanced authentication mechanisms is expected to lead to an overall enhancement of the security posture of 5G-enabled IoT systems. This improvement may include increased resistance to unauthorized access, data breaches, and manipulation. This study demonstrates the efficient integration of advanced authentication mechanisms into the layered architecture of IoT systems. This integration address security concerns at different layers, ensuring a comprehensive security framework. Successful utilization of advanced authentication technologies, such as biometrics, blockchain, or artificial intelligence, are used to showcase their effectiveness in mitigating security risks specific to 5G-connected IoT environments. The implementation of advanced authentication mechanisms is used to reduce the vulnerability of 5G-enabled IoT systems to various types of cyber-attacks, ensuring a more robust defence against threats like identity spoofing, data tampering, and unauthorized access. The research contributes new knowledge to the field of 5G security in IoT, filling gaps in existing literature and providing valuable insights for researchers, practitioners, and policymakers. Overall, the results presented aim to showcase the effectiveness, practicality, and significance of enhancing 5G security in IoT through advanced authentication mechanisms, contributing to the advancement of secure IoT deployments in the era of 5G connectivity.

DISCUSSION

The paper made a discussion on the unique security challenges posed by the combination of 5G and IoT, including the massive number of devices, diverse communication protocols, and varying security capabilities. It also emphasis on the exploration of traditional authentication methods and their limitations in the IoT ecosystem. Hence, it made a discussion on how advanced authentication mechanisms, such as biometrics, multi-factor authentication, and blockchain-based authentication, can enhance security. Most importantly, discussion on the importance of adherence to these standards for interoperability and a consistent security framework. There is also a detailed examination of how advanced authentication mechanisms can be implemented at each layer of the IoT architecture to create a robust security framework. Then the exploration of privacy challenges associated with implementing advanced authentication in 5G IoT. This discussion would likely involve insights from research, industry experts, and practical experiences to provide a comprehensive understanding of the measures needed to enhance 5G IoT security through advanced authentication mechanisms. For future trends, the is a discussion on upcoming trends in 5G IoT security and the potential challenges that may arise.

CONCLUSION

In conclusion, implementing advanced authentication mechanisms in 5G-enabled IoT networks strengthens security significantly. Integrating multi-factor authentication, certificate-based authentication, strong encryption, identity, and access management, zero trust models, and regular security audits achieves a robust security posture, enhancing protection for IoT devices and data. This approach contributes to the overall resilience of 5G networks, effectively mitigating threats and ensuring communication integrity and confidentiality. Prioritizing advanced authentication in the evolving landscape of IoT and 5G is crucial for safeguarding the interconnected ecosystem. This solution significantly improves DDoS attack handling in IoT environments compared to earlier security methodologies. Leveraging 5G capabilities and cutting-edge security measures designed for IoT environments overcomes constraints by 80%, providing a more robust defence against DDoS attacks. With the rise of big data from the Internet of Things, privacy concerns emerge due to potent data mining algorithms. Preserving user privacy, especially sensitive data, is crucial in compliance with IoT rules. Any access control system aiming to earn users' trust must effectively safeguard user privacy.

In summary, further research into IoT privacy needs is needed because privacy regulations must be designed starting with an established model and accompanying development that addresses scalability and the constantly changing setting that defines IoT situations. The is need for establishing public trust and promoting the widespread use of IoT concepts depend heavily on integrating privacy needs from the very beginning of development. There is also a lessons learned from these implementations and potential areas for improvement as a future area of research.

REFERENCES

Aghili, S. F., Mala, H., Schindelhauer, C., Shojafar, M., & Tafazolli, R. (2021). Closed-loop and open-loop authentication protocols for blockchain-based IoT systems. *Information Processing & Management*, *58*(4), 102568. **[Crossref]**

Ahmad, I., Shahabuddin, S., Kumar, T., Okwuibe, J., Gurtov, A., & Ylianttila, M. (2019). Security for 5G and beyond. *IEEE Communications Surveys & Tutorials*, *21*(4), 3682-3722.

Ahmad, R., & Alsmadi, I. (2021). Machine learning approaches to IoT security: A systematic literature review *Internet of Things*, *14*, 100365. **[Crossref]**

Ali, Z. H., Ali, H. A., & Badawy, M. M. (2015). Internet of Things (IoT): definitions, challenges and recent research directions. *International Journal of Computer Applications*, *128*(1), 37-47.

Alsharif, M. H., Jahid, A., Kelechi, A. H., & Kannadasan, R. (2023). Green IoT: A review and future research directions. *Symmetry*, *15*(3), 757.

Amaral, L. A., Hessel, F. P., Bezerra, E. A., Corrêa, J. C., Longhi, O. B., & Dias, T. F. O. (2011). eCloudRFID – A mobile software framework architecture for pervasive RFID-based applications. *Journal of Network and Computer Applications*, *34*(3), 972-979. **[Crossref]**

Benabdessalem, R., Hamdi, M., & Kim, T. H. (2014, 20-23 Dec. 2014). A Survey on Security Models, Techniques, and Tools for the Internet of Things. 2014 7th International Conference on Advanced Software Engineering and Its Applications,

Cerny, T. (2019). Aspect-oriented challenges in system integration with microservices, SOA and IoT. *Enterprise Information Systems*, *13*(4), 467-489. **[Crossref]**https://doi.org/10.1080/17517575.2018.1462406

Datta, P. M. (2022). Strategic Analytics for Decision-Making. In *Global Technology Management 4.0: Concepts and Cases for Managing in the 4th Industrial Revolution* (pp. 91-109). Springer.

Dragoni, N., Giallorenzo, S., Lafuente, A. L., Mazzara, M., Montesi, F., Mustafin, R., & Safina, L. (2017). Microservices: Yesterday, Today, and Tomorrow. In M. Mazzara & B. Meyer (Eds.), *Present and Ulterior Software Engineering* (pp. 195-216). Springer International Publishing. **[Crossref]**

Fan, Q., Chen, J., Deborah, L. J., & Luo, M. (2021). A secure and efficient authentication and data sharing scheme for Internet of Things based on blockchain. *Journal of Systems Architecture*, *117*, 102112. **[Crossref]**

Ghosh, A., Mukherjee, A., & Misra, S. (2021). Sega: Secured edge gateway microservices architecture for iiot-based machine monitoring. *IEEE Transactions on Industrial Informatics*, *18*(3), 1949-1956.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645-1660. **[Crossref]**

Javed, A., Malhi, A., Kinnunen, T., & Främling, K. (2020). Scalable IoT Platform for Heterogeneous Devices in Smart Environments. *IEEE Access*, *8*, 211973-211985. **[Crossref]**

Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the Internet of Things: perspectives and challenges. *Wireless Networks*, *20*(8), 2481-2501. **[Crossref]**

Karie, N. M., Sahri, N. M., & Haskell-Dowland, P. (2020, 21-21 April 2020). IoT Threat Detection Advances, Challenges and Future Directions. 2020 Workshop on Emerging Technologies for Security in IoT (ETSecIoT),

Karie, N. M., Sahri, N. M., Yang, W., Valli, C., & Kebande, V. R. (2021). A Review of Security Standards and Frameworks for IoT-Based Smart Environments. *IEEE Access*, *9*, 121975-121995. **[Crossref]**

Kebande, V. R., Karie, N. M., & Venter, H. (2018). Adding digital forensic readiness as a security component to the IoT domain.

Khanam, S., Ahmedy, I. B., Idris, M. Y. I., Jaward, M. H., & Sabri, A. Q. B. M. (2020). A Survey of Security Challenges, Attacks Taxonomy and Advanced Countermeasures in the Internet of Things. *IEEE Access*, *8*, 219709-219743. **[Crossref]**

Khattak, H. A., Shah, M. A., Khan, S., Ali, I., & Imran, M. (2019). Perception layer security in Internet of Things. *Future Generation Computer Systems*, *100*, 144-164. **[Crossref]**

Kumar, A., Saha, R., Conti, M., Kumar, G., Buchanan, W. J., & Kim, T. H. (2022). A comprehensive survey of authentication methods in Internet-of-Things and its conjunctions. *Journal of Network and Computer Applications*, *204*, 103414. **[Crossref]**

Lai, C., Boi, F., Buschettu, A., & Caboni, R. (2019, 26-28 Aug. 2019). IoT and Microservice Architecture for Multimobility in a Smart City. 2019 7th International Conference on Future Internet of Things and Cloud (FiCloud),

Mirani, A. A., Velasco-Hernandez, G., Awasthi, A., & Walsh, J. (2022). Key Challenges and Emerging Technologies in Industrial IoT Architectures: A Review. *Sensors*, *22*(15).

Moens, P., Bracke, V., Soete, C., Vanden Hautte, S., Nieves Avendano, D., Ooijevaar, T., Devos, S., Volckaert, B., & Van Hoecke, S. (2020). Scalable fleet monitoring and visualization for smart machine maintenance and industrial IoT applications. *Sensors*, *20*(15), 4308.

Piyare, R. (2013). Internet of things: ubiquitous home control and monitoring system using android based smart phone. *International journal of Internet of Things*, *2*(1), 5-11.

Rath, C. K., Mandal, A. K., & Sarkar, A. (2023). Microservice based scalable IoT architecture for device interoperability. *Computer Standards & Interfaces*, *84*, 103697. **[Crossref]**

Said, O., & Masud, M. (2013). Towards internet of things: Survey and future vision. *International Journal of Computer Networks*, *5*(1), 1-17.

Santana, C., Andrade, L., Delicato, F. C., & Prazeres, C. (2021). Increasing the availability of IoT applications with reactive microservices. *Service Oriented Computing and Applications*, *15*(2), 109-126. **[Crossref]**

Sarker, I. H., Khan, A. I., Abushark, Y. B., & Alsolami, F. (2023). Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions. *Mobile Networks and Applications*, *28*(1), 296-312.

Stout, W. M. S., & Urias, V. E. (2016, 24-27 Oct. 2016). Challenges to securing the Internet of Things. 2016 IEEE International Carnahan Conference on Security Technology (ICCST),

Ungurean, I., & Gaitan, N. C. (2020). A software architecture for the Industrial Internet of Things—A conceptual model. *Sensors*, *20*(19), 5603.

Yu, X., & Guo, H. (2019). A survey on IIoT security. 2019 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS),