

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Volume 5, Issue 4, November 2025



# An Approach to Identify the Security of IoT Devices: Challenges and Solution

Rachidatou Fofana, Fatou A Bah, Khushboo Tripathi

Sharda School of Computer Science and Engineering, Sharda University, Greater Noida, UP, India

**Abstract:** The rapid proliferation of Internet of Things (IoT) devices has revolutionized sectors ranging from healthcare and manufacturing to smart homes and cities. However, this expansion introduces significant security vulnerabilities due to the diverse and often resource-constrained nature of IoT devices. Key challenges include weak authentication mechanisms, lack of standardization, insufficient firmware updates, and susceptibility to physical tampering and cyber-attacks such as DDoS, data breaches, and botnets. To address these challenges, various solutions have emerged, including lightweight cryptography, blockchain-based security models, zero-trust architectures, and AI-driven threat detection systems. Moreover, regulatory frameworks and industry standards are evolving to promote security-by-design principles. Emerging trends indicate a shift toward edge computing for realtime threat mitigation, integration of machine learning for anomaly detection, and the adoption of decentralized identity management systems. Ensuring robust IoT security requires a multi-layered, adaptive approach that balances performance, cost, and scalability across heterogeneous devices and networks. Emerging trends indicate a shift toward edge and fog computing, which helps reduce latency and enhances localized security analytics, minimizing the risk associated with centralized vulnerabilities. The adoption of Zero Trust Architecture (ZTA) is on the rise, enforcing detailed access control measures. Additionally, federated learning is facilitating collaborative AI training without revealing raw data. Furthermore, advancements in post-quantum cryptography aim to protect IoT devices against potential threats posed by quantum computing. As the IoT landscape continues to evolve, ensuring end-to-end security presents a dynamic and complex challenge. A combination of robust design principles, adaptive security frameworks, cross-industry collaboration, and continuous innovation is essential to safeguarding IoT environments and securing their full potential.

Keywords: Internet of Things, Lightweight Cryptography, Security Vulnerabilities

#### I. INTRODUCTION

The Internet of Things (IoT) is changing how devices connect and share information. It is used in many areas, such as healthcare, transport, industry, farming, and smart homes. By allowing devices to exchange data in real time, IoT makes automation and efficiency possible.[1]

But this fast growth also brings security problems. Many IoT devices are small, widely spread, and not well protected. This makes them easy targets for cyberattacks. One common threat is the **Distributed Denial of Service (DDoS)** attack.[2] In this case, many hacked devices are used to send too much traffic to a system, blocking real users.

Because IoT devices are numerous and often weak in security, attackers use them for such attacks. A famous example is the **Mirai botnet in 2016**, which disrupted major internet services by exploiting vulnerable IoT devices. [3]This shows how serious the risk can be.

This paper focuses on the **nature**, **mechanics**, **and impact of DDoS attacks** in IoT systems. It also looks at current defence strategies, such as lightweight encryption, stronger device protection, and advanced methods like AI-based intrusion detection or blockchain security. In addition, the paper reviews new trends and future directions, stressing the importance of defences that are scalable, flexible, and proactive. By pointing out vulnerabilities, studying real attack cases, and analysing the latest countermeasures, this research aims to support ongoing efforts to strengthen IoT security.

Copyright to IJARSCT www.ijarsct.co.in







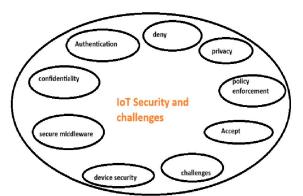
## International Journal of Advanced Research in Science, Communication and Technology

ISO 9001:2015

Impact Factor: 7.67

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Volume 5, Issue 4, November 2025



### II. LITERATURE SURVEY

Authors	Title	Techniques/Algorithm/	Domain	Results	Future gaps
		protocols used and	Specification		
		tools used	1		
Vivek	A	1.Detects threats by	Securing Internet	Lightweight	Developing better
Kumar	lightweight	recognizing patterns of	of Things (IoT)	decision tree IDS	incremental learning
Pandey et	framework	malicious behaviour,	networks, which	enables fast,	to quickly adapt to
al.[4]	to secure	not just fixed	consist of devices	accurate, and	new attack patterns.
	IoT devices	signatures.	with limited	efficient IoT	
	with limited	Incremental Learning	processing power	security with over	
	resources in	Mechanism	and memory.	98% accuracy.	
	cloud	Update its model			
	environmen	incrementally as new			
	ts	attack patterns emerge.			
Neha	A survey on	1.MQTT & CoAP	This review	Machine learning	The review
Sharma et	IoT	(The communication	focuses on the	empowers IoT	identifies future gaps
al. [5]	security:	and security protocols)	domain of IoT	systems by	in Blockchain-IoT
	challenges	2.TLS/DTLS & AMQP	security,	enabling	integration,
	and their	3.LoRa WAN, XMPP,	emphasizing	intelligent threat	including the need
	solutions	IEEE 802.15.4: Used	machine learning	detection,	for adaptable
	using	for wireless	and blockchain	adaptive security	consensus protocols
	machine	communication,	technologies.	policies, and	suited to resource-
	learning and	decentralized sharing,	It explores layered	predictive	constrained devices.
	blockchain	and low-rate personal	IoT architectures,	incident response.	It highlights the lack
	technology	area networks.	smart device	Blockchain	of secure,
		Machine Learning	applications, and	provides a	standardized
		(ML)	secure data	decentralized	methods for
		Blockchain: with	transmission	framework for	software updates and
		consensus algorithm	protocols.	secure	interoperability
		and to automate	The study	communication,	across diverse
		business logic.	highlights how	automating	platforms.
			emerging tech	processes through	Additionally, it calls
			ensures resilience,	smart contracts	for advanced
			privacy, and	and maintaining	intrusion detection,
			intelligent	integrity via	fog ledger

Copyright to IJARSCT www.ijarsct.co.in







ISSN: 2581-9429

## International Journal of Advanced Research in Science, Communication and Technology



 $International\ Open-Access,\ Double-Blind,\ Peer-Reviewed,\ Refereed,\ Multidisciplinary\ Online\ Journal$ 

Volume 5, Issue 4, November 2025

Impact Factor: 7.67

			automation in IoT systems.	consensus algorithms. Together, these technologies create a scalable and resilient infrastructure that defends against evolving cyber threats in connected environments.	protection, and intelligent edge systems using AI and ML.
Asif Ali Laghari et al.[6]	Internet of Things (IoT) applications security trends and challenges	1.machine learning and deep learning for intelligent decision-making, optimization algorithms Raspberry Pi, Node-RED, and Thing Speak. AWS IoT Core and Azure IoT Hub for cloud-based analytics and management. Wireshark, OpenSSL, and Blockchain frameworks.	The domain specification in the review paper includes Smart City, Smart Grid, Smart Health, and Smart Farming, highlighting IoT's role in automating and optimizing diverse sectors. These domains leverage sensor networks, edge computing, and cloud integration to deliver intelligent, responsive services.	IoT security solutions span across network protocols (6LoWPAN, RPL, BLE, ZigBee, LoRaWAN), cloud platforms (Azure, AWS), and encryption methods (ECDH, AES, PKI) to protect data, devices, and communication. Techniques like security analytics, intrusion detection, and biometric authentication help mitigate threats like DoS, eavesdropping, and identity tracking.	Delayed software updates, weak user awareness, and lack of standardized security frameworks, making devices vulnerable to ransomware and remote attacks. Future research must focus on predictive threat detection, secure cloud-to-device communication, and user education to close these critical vulnerabilities.
Thilo Sauter & al.[7]	IoT- Enabled Sensors in Automation Systems and Their Security Challenges	1.IoT systems follow multi-layered architectures (3 to 5 layers), each with distinct roles and security concerns.  2.Security threats span all layers.	IoT specialization domains include smart healthcare, cities, agriculture, industry, and homes—each tailored to optimize data use and	5G-enabled IIoT systems face privacy risks from data tampering, hijacking, and unintended knowledge	Lack of adaptive intrusion detection systems (IDS) capable of monitoring flat, wireless IoT networks and detecting stealthy

Copyright to IJARSCT www.ijarsct.co.in







ISSN: 2581-9429

## International Journal of Advanced Research in Science, Communication and Technology

ISO 9001:2015

 $International\ Open-Access,\ Double-Blind,\ Peer-Reviewed,\ Refereed,\ Multidisciplinary\ Online\ Journal$ 

Volume 5, Issue 4, November 2025

Impact Factor: 7.67

MQTT, CAP, and TLS/DTLS help secure communication, machine learning enhances threat detection. Arduino, Node-RED, and Eclipse ssloT for prototyping and development, alongside cloud platforms. AWS 1oT and Azure 1oT Hub for device management and analytics.  Michae 1 Achieving Mahamat efficient et al.[8] emergy—aware et al.[8] emergy—frace enterowise; a survey of recent solutions and Solutions and Mort Challenges Platform, and Petrokring (SDN), research challenges Platform, and Wireshark for monitoring, anomaly detection, and protocol analysis.  W. M. A. Security—enhanced Wijesunda ret at.1[9] Harborn and Wireshark for monitoring, an omalysis.  W. M. A. Security—enhanced Wijesunda ret at.1[9] Harborn and Grifficant access control mechanisms of treatment of improve safety, efficiency, and reduction making. Users demand stronger energy from vendors, and safeguards against mosaic agai			3.Protocols like	automation.	transfer,	attacks across
TLS/DTLS help secure communication, machine learning enhances threat detection.  Arduino, Node-RED, and Eclipse ssloT for prototyping and development, alongside cloud platforms.  AWS 1oT and Azure IoT Hub for device management and analytics.  Michael 1 Achieving Mahamat et al.[8] energy Transfer (WET), and mobile charging with security in networks: a survey of recent solutions and Virtualization (NFV), and protocols like AWS IoT Device Defender, Armis Agentless Security Platform, and Wireshark for monitoring, anomaly with energy harden integration. like AWS IoT Device Defender, Armis Agentless Security Platform, and Wireshark for monitoring, anomaly detection, and protocol analysis.  W. M. A. Security- B. enhanced wigesum and the communication, machine learning agriculture, and industrial and automation. Users demand stronger rencryption, transparency from vendors, and safeguards agamst mosaic attacks that expose sensitive operational integration. like favore interiments of the communication, and protocols like and Wireshark for monitoring, anomaly detection, and protocol analysis.  W. M. A. Security- B. enthanced protocol analysis.  TLS/DTLS lelp security of into improve safety, and real-time decision-making. Users demand stronger rencryption, rencryption, and safeguards agamst mosaic attacks that expose sensitive operational into support multi-user attacks that expose sensitive operational strospers while the to support multi-user attacks that expose sensitive operational strospers in singlets.  Studies show that lightweight energy on the consumption, using adaptive security design is enercyption and context-aware security, significantly reduce energy to consumption while maintaining adaptive security from a dentry on the protocols, adaptive significantly reduce energy of the protocols, adaptive significantly reduce energy to consumption, using adaptive security from while charging with solutions (e.g., SDN, blockchain, machine learning) adaptive security remains a dediction accurity remains a distinct or pro					· ·	
communication, machine learning enhances threat detection. Arduino, Node-RED, and Eclipse ssloT for prototyping and development, alongside cloud platforms.   AWS IoT and Azure IoT Hub for device management and analytics.   Michael 1 (EH), Wireless Energy et al. [8] energy—aware security in IoT notoworks: a survey of recent solutions and protocol shallenges   Networking (SDN), and protocols like MQTT and blockchain, like AWS IoT Device Defender, Armis Agentless Security Platform, and Wireshark for monitoring, anomaly detection, and protocol analysis.   W. M. A. Security—and notice thanks of monitoring, anomaly detection, and protocol analysis.   Internet of Things (Internet of Things) the machine learning) and enhanced with earning to improve safety, efficient, caretyling fictione, and real-time decision—making. Users demand stronger encryption, transparency from vendors, and safeguards against mosaic attacks that expose sensitive operation attacks that expose sensitive operation and insights.   Internet of Studies show that lightweight encryption and adaptive security significantly reduce energy consumption and adaptive security significantly reduce energy consumption while maintaining adequate methods.   Software-Defined Networking (SDN), blockchain, like AWS IoT Device Defender, Armis Agentless Security endet to balance of the protocol analysis.   Internet of Things of the protocol analysis.   Internet of Things on the protocol and threat-aware security without as smart cities, agriculture, and industrial systems.   Internet of Things on the protocol and threat-aware security with energy barvesting, offer dynamic security with energy barvesting, offer dynamic security with energy barvesting, offer dynamic security without compromising and threat-aware set of the protocol and threat-aware set of the protocol and threat-aware set of the protocol and threat-aware security with protocol analysis.   Internet of Things on the protocol				,	*	•
machine learning enhances threat detection. Arduino, Node-RED, and Eclipse ssIoT for prototyping and development, alongside cloud platforms.  AWS IoT and Azure IoT Hub for device management analytics.  Michael Achieving et al.[8] aware et al.[8] aware solutions and solutions and protocol is key with challenges  Michael Achieving hammat et al.[8] aware border centry of recent solutions and mobile charging with route planning to extend device lifetime. Persearch challenges  Morthage Alebased methods.  Networking (SDN), Network Function challenges  Morthage Agentless Security, Platform, and Wireshark for monitoring, anomaly detection, and protocol analysis.  My. M. A. Security— I. Secure IoT firmware updates using IoTA, IPFS, and a validating Wijesunda Wijesunda firmware updates wing and wijesunda wijesunda firmware updates using IoTA, IPFS, and a validating Wijesunda firmware updates wing serving protocol and safeguards against mosaic attacks that expose sensitive operational insights. and asfeguards against mosaic attacks that expose sensitive operational insights. The protocols against mosaic attacks that expose sensitive operational insights. The protocols against mosaic attacks that expose sensitive operational insights. The protocols against mosaic attacks that expose sensitive operational insights. The protocols against mosaic attacks that expose sensitive operational insights. The protocols against mosaic attacks that expose sensitive operational insights. The protocols against mosaic attacks that expose sensitive operational insights. The protocols against mosaic attacks that expose sensitive operational insights. The protocols against mosaic attacks that expose sensitive operational insights. The protocols against mosaic attacks that expose sensitive operational insights. The protocols against mosaic attacks that expose sensitive operational insights. The protocols against mosaic attacks that expose sensitive operational insights. The protocols against mosaic attacks that expose sensitive operational ins			_			
enhances threat detection. Arduino, Node-RED, and Eclipse ssloT for prototypring and development, alongside cloud platforms. AWS IoT and Azure IoT Hub for device management and analytics.  Michae1 Achieving Mahamat efficient et al.[8] energy—aware survey of recent solutions and Networking and holoschain, integration. Challenges Virtualization (NFV), and protocols like MQTT and blockchain, integration. like AWS IoT Device Defender, Armis Agentless Security Platform, and Wireshark for monitoring, anomaly, detection, and protocol analysis.  W. M. A. Security—B. enhanced Witesanda Wijesunda Wijesunda Wijesunda Ifirmware Update wing standard very lower of the management and davelopment, alongside cloud platforms. AWS IoT Device parameter and analytics.  Securing IoT and Extreme decision-making. transfer underdeveloped against mosaic attacks that expose sensitive operations attacks that expose sensitive operations attacks that expose sensitive operations of statucks that expose sensitive operations of substances and networks while minimizing energy mobile charging with route planning to extend device lifetime. lightweight reduce energy consumption and adaptive security, significantly reduce energy consumption and adaptive security significantly reduce energy consumption and adaptive security. and context-aware security, and solutions (e.g., SDN, blockchain, mitegration. like AWS IoT Device Defender, Armis Agentless Security Platform, and Wireshark for monitoring, anomaly detection, and protocol analysis.  W. M. A. Security—B. enhanced with a cloud transparency from vendors, and against mosaic attacks that expose sensitive operations adaptive security significantly reduce energy consumption, adequate encryption and adaptive security significantly reduce energy consumption, especially in trusted consumption adequate encryption and adaptive security with energy of the planning integration. It with the consumption of the planning integration. It with the energy of the planning integration. It with the energy of the plann			· ·			
detection. Arduino, Node-RED, and Eclipse ssloT for prototyping and development, alongside cloud platforms.  AWS 1oT and Azure 1oT Hub for device management and analytics.  Michae 1 Achieving et al.[8] efficient et al.[8] energy—avare scurrity in 1otvorks: a survey of recent solutions and networking (SDN), research challenges  Mothalenges  Michae 1 Achieving et al.[8] (EH), Wireless Energy—trute planing to extend device lifetime. networks: a survey of recent solutions and management end and mobile charging with recent solutions and protocols like MQTT and blockchain, integration. like AWS 1oT Device Defender, Armis Agentless Security Platform, and Wireshark for monitoring, anomaly detection, and protocol analysis.  W. M. A. Security—B. M. A. Security—B. management under a vigile susing IOTA, liPFS, and a validating Wijesunda Wijesunda firmware understands and vevelopment, alongside cloud platform prototyping and development, alongside cloud platform prototyping and development, alongside cloud platforms. AWS 1oT Device Defender, Armis Agentless Security are increasingly with energy machine learning systems.  W. M. A. Security—B. energy—Interventing and protocols like aware and protocol analysis.  The security and and context-aware solutions (e.g., SDN, blockchain, methical carning-based solutions (e.g., SDN, blockchain, methical carning-bas						
Arduino, Node-RED, and Eclipse ssloT for prototyping and development, alongside cloud platforms.  AWS IoT and Azure IoT Hub for device management and analytics.  Michae¹ Achieving efficient ctal[8] efficient ctal[8] recent solutions assuring mobile charging with security in IoT networks: a survey of recent solutions and notocols like MQTT and blockchain integration. like AWS IoT Device Defender, Armis Agentless Security Platform, and Wireshark for monitoring, anomaly detection, and protocol analysis.  W. M. A. Security—B. M. A. Security—B. who has a safeguards against mosaic attacks that expose sensitive operational insights.  Securing IoT networks while expose sensitive operational insights.  Securing IoT networks while lightweight minimizing energy consumption, using adaptive security significantly reduce energy protection with minimal energy consumption while maintaining adaptive security balance robust protection with minimal energy consumption while maintaining adequate energy harvesting-based security. Cross-layer frameworks and protocols like MQTT and blockchain integration. like AWS IoT Device Defender, Armis Agentless Security Platform, and Wireshark for monitoring, anomaly detection, and protocol analysis.  W. M. A. Security—B. M. A. Security—B. and protocol analysis.  Internet of Thus to support the charge with energy with energy with energy levels that extend device and device management and and without as smart cities, agriculture, and industrial systems.  Internet of Things (IoT), Security and firmware updates security energy without as smart cities, agriculture, and industrial systems.  Imagentary design is still underdeveloped mentphodos. Sadaptive energy brotection, while maintaining adequate energy brotection, while maintaining adequate energy brotection, and trusted environments. Context-aware solutions (e.g., SDN, blockchain, machine learning) are increasingly are increasingly are increasingly are increasingly are increasingly				• .	_	
and Eclipse ssloT for prototyping and development, alongside cloud platforms.  AWS IoT and Azure IoT Hub for device management and analytics.  Michae1 Achieving efficient energy-aware energy-aware security in IoT networks: a survey of recent solutions and protocols like MQTT and blockchain integration. Ike AWS IoT Device Defender, Armis Agentless Security Platform, and Wireshark for monitoring, anomaly detection, and protocol analysis.  Michae1 Achieving efficient energy-aware energy-aware energy-aware security in IoT networks: a survey of recent solutions and protocols like MQTT and blockchain integration. Ike AWS IoT Device Defender, Armis Agentless Security Platform, and Wireshark for monitoring, anomaly detection, and protocol analysis.  W. M. A. Security-Band and firmware whale enhanced wijesunda firmware of the Achieving from the Achieving firmware in the Achieving and consumption and analytics.  Security operation, against mosaic attacks that expose sensitive operational insights.  attacks that expose sensitive operational insights.  Studies show that lightweight encryption and adaptive security significantly reduce energy protocols, adaptive reduce energy brotocols, adaptive reduce energy while maintaining security of security, and energy harvesting-based security. Cross-layer tracked environments.  Al-powered with energy firmware without as smart cities, agriculture, and industrial systems.  W. M. A. Security-Band availidating firmware updates integration, update integration, update integration, update integration in the protocol of the minimizing energy consumption, using to adopt recent without adequate energy harvesting-based security. The protocols adaptive recurity with energy introduce energy protocols, adaptive recurity adaptive security in energy harvesting-based security. Specific energy and adoptive security with energy introduce of the protocols adaptive security in entwork in minimizing energy consumption adaptive security with energy introduce energy while maintaining security in energy in						
michael Achieving energy- et al.[8] energy- survey of recent solutions and protocols and protocols and protocols and protocols and protocols like MQTT and blockchain integration. like AWS IoT Device Defender, Armis Agentless Security platform, and Wireshark for monitoring, anomaly detection, and protocol analysis.    michael Achieving (SDN), research challenges   Networking (SDN), and protocols analysis.   Security security with energy efficient eleming) are increasingly are increasingly are increasingly with energy detection, and protocol analysis.   Security and device lot firme.   SDN, blockchain, argireluture, and moles for omonitoring, anomaly detection, and protocol analysis.   Security and gaanst mosaic attacks that expose sensitive operational matacks that expose sensitive operational insights.   Studies show that expose sensitive operational minisights.   Studies show that expose sensitive operational matacks that expose security significantly expose occurity se			· · ·	making.	•	
development, alongside cloud platforms.  AWS IoT and Azure IoT Hub for device management and analytics.  Michae¹ Achieving Harvesting et al.[8] ergy energy energy aware security in networks: a survey of recent solutions and Protocols and protocols like MQTT and blockchain integration.  Network Function Defender, Armis Agentless Security Agentless Security and protocols like MQTT and blockchain integration.  Ike AWS IoT Device Defender, Armis Agentless Security and moritoring, anomaly detection, and protocol analysis.  W. M. A. Security-  W. M. A. Security- B. enhanced Wijesunda firmware updates wing and analytics.  Michae¹ Achieving (SDN), Natwork Function and protocols like as smart cities, agriculture, and industrial systems.  AWS IoT and Azure expose sensitive operational attacks that expose sensitive volunerable to unauthorized access.  Scuring IoT studies show that networks while lightweight reduce energy encryption and adaptive security significantly reduce energy consumption with entition and adaptive security significantly reduce energy consumption with energy harvesting based security.  Network Function (NFV), and adaptive sucurity, and energy harvesting based security.  Network Function (NFV), and and protocols like MQTT and blockchain integration.  Ike AWS IoT Device Defender, Armis Agentless Security with energy large increasingly are increasingly and threat-aware security remains a challenge—future research should focus on optimizing machine learning based security with energy levels that extend entergence in the protocol analysis.  W. M. A. Security-  B. enhanced with analytics.  Michae¹ Defender,			_		·	* *
cloud platforms. AWS 1of and Azure IoT Hub for device management and analytics.  Michae 1 Mahamat et al.[8]  Michae 1 Mahamat et al.[8]  Achieving Gifficient networks: a survey of recent solutions and Networking Challenges  Network Function Challenges  Network Function Virtualization (NFV), and protocols lick MQTT and blockchain integration.  Network Function Virtualization (NFV), and protocols lick MQTT and blockchain integration.  Network Function Virtualization (NFV), and protocols lick MQTT and blockchain integration.  Network for monitoring, anomaby detection, and protocol analysis.  W. M. A. Security B.  wh. M. A. Security B.  cloud platforms. AWS 1of and Azure IoT Hub for device management and analytics.  Securing IoT networks while minimizing energy consumption, using rotocous, adaptive security significantly significantly reduce energy protection with minimal energy consumption, especially in trusted consumption, sepecially in trusted consumption, using adaptive security significantly reduce energy protection with minimal energy consumption, sepecially in trusted consumption, using adaptive security significantly reduce energy by reduce energy harvesting. SDN, blockchain, integration.  Ilike AWS 1oT Device Defender, Armisi and with consumption and context-aware security, and integration (NFV), and protocols lick MQTT and blockchain integration.  Wireshark for monitoring, anomaby efficiency across diverse IoT applications such without as smart cities, agriculture, and industrial systems.  W. M. A. Security B.  wh. M. A. Security- B. enhanced Wijesunda  clockers while lightweight inctworks while intervely with consumption, using recry consumption, using adaptive security significantly reduce energy of future solutions must balance robust institution, energy adaptive security security significantly reduce energy of future solutions must balance robust institution.  Energy-aware security and context-aware solutions must balance robust institution.  Cross-layer frameworks and context-aware solutions must ba					_	
AWS IoT and Azure IoT Hub for device management and analytics.  Michae1 Achieving efficient ct al.[8] energy—aware security in IoT networks a survey of recent solutions and protocols like MQTT and blockchain integration. like AWS IoT Device Defender, Armis Agentless Security Plafform, and Wireshark for monitoring, anomaly detection, and protocol analysis.  W. M. A. Security—B. County in IoT Hub for device management and analytics.  Michae1 Achieving efficient ct al.[8] efficient and solutions and protocols like MQTT and blockchain integration. like AWS IoT Device Platform, and Wireshark for monitoring, anomaly detection, and protocol analysis.  W. M. A. Security—B. embanced will select a significantly reduce energy balance robust reduce energy while maintaining adaquate energy harvesting, based security. Cross-layer frameworks and Al-powered solutions (e.g., SDN, blockchain, integration. like AWS IoT Device Platform, and Wireshark for monitoring, anomaly detection, and protocol analysis.  W. M. A. Security—B. embanced with energy enarce in trusted environments. Context-aware solutions (e.g., SDN, blockchain, integration and minimal energy consumption, using toconsumption adaptive security with energy independent entworks while lightweight enconsumption, using dacquate energy harvesting, and context-aware solutions (e.g., SDN, blockchain, integration and adaptive security with energy balance robust reduce energy to consumption, using dacquate energy in trusted in trusted environments. Context-aware security remains a challenge—future research should for applications such as smart cities, agriculture, and industrial systems.  W. M. A. Security—B. Security—B. Energy—aware indeptive security design is security in entworks and context-aware solutions (e.g., SDN, blockchain, integration and wither all protection with ene					against mosaic	privilege separation,
Michae1			cloud platforms.		attacks that	leaving systems
Michae1   Achieving   1.Energy Harvesting   (EH), Wireless Energy   networks   while   minimizing energy   consumption, using   still underdeveloped   dadptive   security   still underdeveloped   dadptive   security   still underdeveloped   still underdeveloped   dadptive   securi			AWS IoT and Azure		expose sensitive	vulnerable to
Michae 1 Achieving (EH), Wireless Energy et al.[8] energy- energy- energy of recent solutions and Networks (Sallenges) (EH), Wireless Energy extend device lifetime. networks: a part of recent solutions and Network Function challenges (SDN), research challenges (SDN), research (SH) (ST), and protocols like MQTT and blockchain integration. like AWS IoT Device Defender, Armis Agentless Security Platform, and Wireshark for monitoring, anomaly detection, and protocol analysis.  W. M. A. Security- B. enhanced (W. A. Security- B. enhanced Wijesunda (Im) (Im) (Im) (Im) (Im) (Im) (Im) (Im)			IoT Hub for device		operational	unauthorized access.
Michae¹ Achieving Mahamat efficient ct al.[8] energy aware officient aware security in lo IoT extend device lifetime. networks: a survey of recent solutions and mobile charging with solutions and protocols like MQTT and blockchain integration. like AWS IoT Device Defender, Armis Agentless Security Platform, and Wireshark for monitoring, anomaly detection, and protocol analysis.  W. M. A. Security—B. enhanced Wijesunda aware  W. M. A. Security—B. enhanced Wijesunda aware  W. M. A. Security—B. enhanced Wijesunda aware  I. Energy Harvesting in tetworks while lightweight networks while lightweight enctyption and adaptive security significantly protocols, adaptive security with enimizing energy and context-aware security, and energy harvesting-based security. Cross-layer trusted environments. Context-aware solutions (e.g., SDN, blockchain, machine learning) combined with energy harvesting, offer dynamic security with energy levels that extend device and networks while lightweight encryption and adaptive security significantly protocols, adaptive consumption onsumption, using adequate especially in consumption, especially in frameworks and threat-aware solutions (e.g., SDN, blockchain, machine learning) combined with energy levels that extend device and of device and network lifetime entry without compromising asfety. Internet of Things affety. Internet of Things affety. Internet of Things affety. Internet of Things aware onsumption, using adaptive security while maintaining adequate especially in trusted environments. Context-aware security remains a challenge—future research should focus on optimizing nergy while maintaining adequate environments. Context-aware security especially in trusted environments. Context-aware security of the energy based security. SDN, blockchain, machine learning of the energy based security. SDN, blockchain, machine learning of the energy based security. SDN, blockchain, machine learning of the energy based security. SDN, blockchain, machine learning of the energy based security to trea			management and		insights.	
Mahamat et al. [8] (EH), Wireless Energy more and aware mobile charging with security in IoT motte planning to extend device lifetime. networks: a survey of recent solutions and Networking (SDN), research challenges (Challenges Platform, and integration. like AWS IoT Device Defender, Armis Agentless Security Platform, and Wireshark for monitoring, anomaly detection, analysis.  W. M. A. Security-  W. M. A. Security- B. enhanced Wijesunda   Wijesunda   Gifficient energy- mobile charging with route planning to entropy mobile charging with route planning to energy indiving adaptive security significantly reduce energy protocols, adaptive and consumption, using adaptive security significantly reduce energy protocols, adaptive and context-aware security, and ado context-aware security. Transfer (WET), and consumption, using adaptive security significantly reduce energy protocols, adaptive and context-aware security. Transfer (WET), and consumption, using adaptive security significantly reduce energy protocols, adaptive security, and adaptive security significantly reduce energy protocols, adaptive and consumption and consumption, using adaptive security significantly reduce energy protocols, adaptive security, and adoptor consumption and consumption, using adaptive security significantly reduce energy protocols, adaptive security, and consumption, using adaptive security significantly reduce energy protocols, adaptive security, and consumption, using adaptive security significantly reduce energy protocols, adaptive security, and consumption, using adaptive security significantly reduce energy protocols, adaptive security, and consumption and consumption, using adaptive security in trouve energy protocols, adaptive security, and consumption and consumption. The protocol is adaptive security.  Tarsfer (WET), and consumption, using adaptive security in consumption.  Software-Defined Networking (SDN), research (Networking (SDN), hotochain, machine learning) are increasingly with energy dequate and threat-aware solutions			analytics.			
Mahamat et al. [8] (EH), Wireless Energy more and aware mobile charging with security in IoT motte planning to extend device lifetime. networks: a survey of recent solutions and Networking (SDN), research challenges (Challenges Platform, and integration. like AWS IoT Device Defender, Armis Agentless Security Platform, and Wireshark for monitoring, anomaly detection, analysis.  W. M. A. Security-  W. M. A. Security- B. enhanced Wijesunda   Wijesunda   Gifficient energy- mobile charging with route planning to entropy mobile charging with route planning to energy indiving adaptive security significantly reduce energy protocols, adaptive and consumption, using adaptive security significantly reduce energy protocols, adaptive and context-aware security, and ado context-aware security. Transfer (WET), and consumption, using adaptive security significantly reduce energy protocols, adaptive and context-aware security. Transfer (WET), and consumption, using adaptive security significantly reduce energy protocols, adaptive security, and adaptive security significantly reduce energy protocols, adaptive and consumption and consumption, using adaptive security significantly reduce energy protocols, adaptive security, and adoptor consumption and consumption, using adaptive security significantly reduce energy protocols, adaptive security, and consumption, using adaptive security significantly reduce energy protocols, adaptive security, and consumption, using adaptive security significantly reduce energy protocols, adaptive security, and consumption, using adaptive security significantly reduce energy protocols, adaptive security, and consumption and consumption, using adaptive security in trouve energy protocols, adaptive security, and consumption and consumption. The protocol is adaptive security.  Tarsfer (WET), and consumption, using adaptive security in consumption.  Software-Defined Networking (SDN), research (Networking (SDN), hotochain, machine learning) are increasingly with energy dequate and threat-aware solutions	Michae'1	Achieving	1.Energy Harvesting	Securing IoT	Studies show that	Energy-aware
eral.[8] energy- aware mobile charging with route planning to extend device lifetime. networks: a solutions and methods. solutions and protocols like MQTT and blockchain integration. like AWS IoT Device Defender, Armis Agentless Security Platform, and Wireshark for monitoring, anomaly detection, and protocol analysis.  W. M. A. Security- B. enhanced Wijesunda firmware  weigh aware mobile charging with route planning to planning to extend device lifetime. extend device lifetime. protocols, adaptive security significantly significantly significantly significantly significantly significantly significantly significantly and context-aware security, and energy harvesting-based security. Cross-layer trusted consumption with energy and context-aware security, and energy harvesting-based security. Cross-layer trusted trusted environments. Context-aware solutions (e.g., SDN, blockchain, machine learning) to consumption, using significantly significantly significantly adaptive security with energy while maintaining adequate especially in trusted trusted environments. Context-aware solutions (e.g., SDN, blockchain, machine learning) to based security. Cross-layer trusted environments. Context-aware solutions (e.g., SDN, blockchain, machine learning) to based security environments. Context-aware solutions (e.g., SDN, blockchain, machine learning) to based security environments. Lightweight trusted trusted environments. Context-aware solutions (e.g., SDN, blockchain, machine learning) to based security environments. Context-aware solutions (e.g., SDN, blockchain, machine learning) to batteryless or ultra-specially in trusted environments. Context-aware solutions or especially in trusted environments. Context-aware solutions (e.g., SDN, blockchain, machine learning) to based security environments. Lightweight trusted environments. Context-aware solutions (e.g., systems, when the energy divided to balance robust in trusted trusted environments. Context-aware solutions (e.g., systems, when the energy with energy divided to the	Mahamat	efficient		networks while	lightweight	security design is
aware security in route planning to lot extend device lifetime. networks: a 2.For security, they survey of adopt AI-based recent solutions 3.Software-Defined and Networking (SDN), research Network Function challenges WiTtualization (NFV), and protocols like MQTT and blockchain integration. like AWS IoT Device Defender, Armis Agentless Security Platform, and Wireshark for monitoring, anomaly detection, and protocol analysis.  W. M. A. Security- mobile charging with route planning to extend device lifetime. extend device lifetime. lightweight protocols, adaptive and context-aware security. The protection with minimal energy while maintaining adequate especially in trusted consumption, especially in trusted Lightweight consumption, especially in trusted Lightweight consumption, especially in trusted Lightweight rusted Solutions (e.g., SDN, blockchain, machine learning) are increasingly used to balance robust security with energy efficiency across diverse 10T applications such as smart cities, agriculture, and industrial systems.  W. M. A. Security- enhanced wijesunda firmware updates using 10TA, Wijesunda firmware IPFS, and a validating Firmware Update in trusted learning to consumption with gignificantly reduce energy consumption with lightweight reduce energy consumption, especially in trusted Lightweight consumption, especially in trusted Lightweight trusted security. Cross-layer frameworks and context-aware solutions (e.g., SDN, blockchain, machine learning) are increasingly used to balance robust security. Cross-layer frameworks and context-aware solutions (e.g., SDN, blockchain, machine learning) are increasingly used to balance robust in trusted energy protection while maintaining adequate especially in trusted Lightweight consumption, especially in trusted Lightweight reduce energy consumption, especially in trusted Lightweight reduce energy protection, especially in trusted Lightweight energy systems, when combined with energy with energy officiency are increasingly used to balance observed the protection	et al.[8]	energy-	Transfer (WET), and	minimizing energy	encryption and	still underdeveloped
security in lot extend device lifetime. Extend lifetime extend device lifetime. Extend lifetime extend lifetime extend lifetime extend lifetime and context-aware security. Extend lifetime extend lifetime extend lifetime environments without extend lifetime and industrial systems. Extend lifetime without extend lifetime and industrial systems. Extend lifetime without extend lifetime environments lifetime without extend lifetime environments lifetime without extend lifetime environments lifetime without extend lifetime and industrial systems. Extend lifetime without extend lifetime environments lifetime without extend lifetime environments lifetime environments lifetime without extend lifetime environments lifetime environments lifetime environments lifetime environments lifetime environments lifetime environments lifetime environments. Combined with energy with energy lifetime energy and industrial systems. Extend lifetime environments lifetime environments lifetime environments lifetime environments. Combined with environments extend environments					* *	•
IoT networks: a survey of recent methods.  Solutions and Networking (SDN), research Network Function challenges  MQTT and blockchain integration.  Iike AWS IoT Device Defender, Armis Agentless Security and Wireshark for monitoring, anomaly detection, and protocol analysis.  W. M. A. Security-  W. M. A. Security-  B. Wijesunda with a dopt adopt AI-based methods.  Iot of recent metworks: a survey of recent methods.  Iightweight protocols, adaptive and context-aware security, and and context-aware security in trusted environments.  Consumption while maintaining adequate especially in trusted convironments.  Context-aware systems, when combined with focus on optimizing nandhine learning are increasingly are		security in	route planning to			balance robust
networks: a survey of recent survey of recent solutions adopt AI-based methods.  solutions and solutions and protocols like MQTT and blockchain integration. like AWS IoT Device Defender, Armis Agentless Security Platform, and Wireshark for monitoring, anomaly detection, and protocol analysis.  W. M. A. Security-  W. M. A. Security-  Wijesunda Wineshared  Wijesunda Wineshared  Wijesunda Wineshared  Wijesunda Wineshared  Wineshared  Wijesunda Wineshared  Wijesunda Wijesunda Wineshared  Solutions (2.For security, they adopt AI-based and context-aware security, and energy harvesting-based security. Cross-layer  Cross-layer  Intrusted energy harvesting-based security. Trusted energy in trusted environments. Learning-based security remains a challenge—future research should focus on optimizing and energy with energy especially in trusted environments. Context-aware systems, when combined with focus on optimizing with energy dynamic security levels that extend device and network lifetime without compromising safety.  Wijesunda		_		•		protection with
survey of recent methods.  solutions 3.Software-Defined Networking (SDN), research Challenges Virtualization (NFV), and protocols like MQTT and blockchain integration.  like AWS IoT Device Defender, Armis Agentless Security Platform, and Wireshark for monitoring, anomaly detection, and protocol analysis.  W. M. A. Security-B.  W. M. A. Security- B.  while maintaining adequate especially for protection, especially in trusted Lightweight learning-based security. Cross-layer frameworks and and protocols like MQTT and blockchain integration.  like AWS IoT Device Defender, Armis Agentless Security Platform, and Wireshark for monitoring, anomaly detection, and protocol analysis.  W. M. A. Security-B.  wineshare methods.  3.Software-Defined energy harvesting-based security. Cross-layer frameworks and and protocols like have solutions (e.g., SDN, blockchain, machine learning) are increasingly used to balance robust security with energy efficiency across device and diverse IoT applications such as smart cities, agriculture, and industrial systems.  W. M. A. Security-B.  without compromising safety.  Internet of Things Secure, efficient firmware updates on low-power IoT speed, and security speed integration, update specially in trusted trusted environments. Context-aware solutions (e.g., SDN, blockchain, machine learning, batch framework security energy and trusted environments. Context-aware solutions (e.g., SDN, blockchain, machine learning, batch framework security denvironments se				~ ~	0,3	*
recent solutions and research challenges					*	0,
solutions and Networking (SDN), research challenges  Network Function Virtualization (NFV), and protocols like MQTT and blockchain integration. like AWS IoT Device Defender, Armis Agentless Security Platform, and Wireshark for monitoring, anomaly detection, and protocol analysis.  W. M. A. Security-B. wijesunda firmware with and wijesunda firmware incasting and protocol in the solutions (SDN), based security. Cross-layer frameworks and Al-powered solutions (e.g., SDN, blockchain, machine learning) to cross-layer frameworks and and protocols like AWS IoT Device solutions (e.g., SDN, blockchain, machine learning) are increasingly used to balance officiency across diverse IoT applications such as smart cities, agriculture, and industrial systems.  W. M. A. Security-B. enhanced wijesunda firmware updates firmware integration and protocol integration integration integration integration (NFV), and protocol solutions (e.g., SDN, blockchain, machine learning) to combined with focus on optimizing offer dynamic security dynamic security envit environments device and industrial systems.  W. M. A. Security-B. enhanced wijesunda firmware updates integration, update integration, update integration, update integration, integration integration, integration integ		_	_		_	- '
and research challenges  Network Function Virtualization (NFV), and protocols like MQTT and blockchain integration. like AWS IoT Device Defender, Armis Agentless Security Platform, and Wireshark for monitoring, anomaly detection, and protocol analysis.  W. M. A. Security-B. wijesunda  wind protocols like AWS IoT Device Defender, Armis Agentless Security Platform, and wijesunda  wind protocols like AI-powered solutions (e.g., SDN, blockchain, machine learning) are increasingly used to balance robust security with energy with energy agriculture, and industrial systems.  w. M. A. Security-enhanced wijesunda  wijesunda  notwork Function Cross-layer frameworks and AI-powered solutions (e.g., SDN, blockchain, machine learning) are increasingly used to balance robust security with energy with energy with energy environments device and device and industrial systems.  w. M. A. Security-enhanced wijesunda  wijesunda  Network Function Cross-layer frameworks and trusted environments. Context-aware security remains a challenge—future research should focus on optimizing machine learning harvesting, offer devices that extend device and device and evice and industrial systems.  Internet of Things Secure, efficient firmware updates on low-power IoT speed, and security speed, and security				•	_	
research challenges  Network Function Virtualization (NFV), and protocols like MQTT and blockchain integration.  like AWS IoT Device Defender, Armis Agentless Security Platform, and Wireshark for monitoring, anomaly detection, and protocol analysis.  W. M. A. Security-B. enhanced Wijesunda  Wijesunda  Research challenges  Network Function (NFV), frameworks and Al-powered solutions (e.g., SDN, blockchain, machine learning) and threat-aware systems, when combined with focus on optimizing machine learning harvesting, offer dynamic security with energy efficiency across diverse IoT applications such as smart cities, agriculture, and industrial systems.  Network Function (NFV), frameworks and Al-powered solutions (e.g., SDN, blockchain, machine learning) are increasingly used to balance robust security with energy efficiency across diverse IoT applications such as smart cities, agriculture, and industrial systems.  Network Function (NFV), and protocols like MQTT and blockchain solutions (e.g., SDN, blockchain, machine learning) and threat-aware systems, when combined with focus on optimizing machine learning harvesting, offer dynamic security environments without constrained environments without compromising safety.  Itrusted environments.  Context-aware and threat-aware systems, when combined with energy energy machine learning harvesting, offer dynamic security environments without compromising safety.  Itrusted environments.  Context-aware and threat-aware systems, when combined with energy dynamic security energy without constrained environments without compromising safety.  Itrusted environments.  Context-aware and threat-aware systems, when combined with energy dynamic security diverse and increasingly are increasingly are increasingly and threat-aware systems, when combined with energy dynamic security of the dynamic sec					*	•
challenges  Virtualization (NFV), and protocols like AI-powered solutions (e.g., and threat-aware integration.  like AWS IoT Device Defender, Armis Agentless Security Platform, and Wireshark for monitoring, anomaly detection, and protocol analysis.  W. M. A. Security-B. enhanced Wijesunda  Wijesunda  Challenges  Virtualization (NFV), and protocols like AI-powered solutions (e.g., and threat-aware solutions (e.g., and threat-aware systems, when machine learning) security remains a challenge—future research should focus on optimizing machine learning harvesting, offer dynamic security divamic security levels that extend device and network lifetime without compromising agriculture, and industrial systems.  Ilearning-based security remains a challenge—future research should focus on optimizing machine learning machine learning harvesting, offer dynamic security diverse IoT applications such as smart cities, agriculture, and industrial systems.  W. M. A. Security-  B. enhanced updates using IOTA, IPFS, and a validating Firmware Update  Vijesunda  Virtualization (NFV), AI-powered solutions (e.g., and threat-aware challenge—future research should focus on optimizing machine learning harvesting, offer dynamic security with energy levels that extend device and metwork lifetime without compromising detection accuracy.  SDN, blockchain, machine learning harvesting, offer dynamic security without constrained environments without compromising safety.  SDN, blockchain, machine learning harvesting, offer dynamic security without constrained environments without compromising safety.  SDN, blockchain, machine learning harvesting, offer dynamic security without constrained environments without compromising safety.  SDN, blockchain, machine learning harvesting, offer dynamic security constrained environments without compromising safety.  SDN, blockchain, machine learning harvesting, offer dynamic security occurrence without compromising safety.  SDN and threat-aware combined with energy dynamic security occurrence without comprom			- , , , , , , , , , , , , , , , , , , ,	-	*	•
and protocols like MQTT and blockchain integration.  like AWS IoT Device Defender, Armis Agentless Security and Wireshark for monitoring, anomaly detection, and protocol analysis.  W. M. A. Security-B.  with and protocols like MQTT and blockchain integration.  like AWS IoT Device Defender, Armis Agentless Security and Wireshark for monitoring, anomaly detection and protocol analysis.  Al-powered solutions (e.g., solutions) (e.g., and threat-aware and threat-aware systems, when research should combined with focus on optimizing machine learning harvesting, offer dynamic security dynamic security with energy levels that extend device and network lifetime without compromising safety.  W. M. A. Security-B.  Wijesunda firmware updates using IOTA, IDT) (IOT) Security and IPFS, and a validating Firmware Update on low-power IoT speed, and security				· ·		
MQTT and blockchain integration.  like AWS IoT Device Defender, Armis Agentless Security Platform, and Wireshark for monitoring, anomaly detection, and protocol analysis.  W. M. A. Security-B. wijesunda firmware Wijesunda firmware Integration.  Ike AWS IoT Device Defender, Armis Agentless Security and firmware Internet of Things SDN, blockchain, machine learning) combined with focus on optimizing machine learning machine learning harvesting, offer dynamic security dynamic security dynamic security environments with energy levels that extend device and diverse IoT network lifetime without compromising detection accuracy.  I.Secure IoT firmware Internet of Things Secure, efficient speed, and security integration, update speed, and security speed, and security on low-power IoT speed, and security speed, and security		chancinges	` '			_
integration.  like AWS IoT Device Defender, Armis Agentless Security Platform, and Wireshark for monitoring, anomaly detection, and protocol analysis.  W. M. A. Security- B. enhanced Wijesunda firmware    Mighapeta   Mighapeta			_	*		•
like AWS IoT Device Defender, Armis Agentless Security Agentless Security Platform, and Wireshark for monitoring, anomaly detection, and protocol analysis.  W. M. A. Security Wigesunda firmware    Iike AWS IoT Device Defender, Armis are increasingly are increasingly used to balance robust security used to balance of the increasingly harvesting, offer dynamic security dynamic security constrained environments without network lifetime without compromising safety.    Water and industrial systems   Internet of Things   Secure, efficient firmware updates on low-power IoT			*	` •		•
Defender, Armis Agentless Security used to balance Platform, and Wireshark for monitoring, anomaly detection, and protocol analysis.  W. M. A. Security Wigsunda firmware  Defender, Armis Agentless Security used to balance platform, and with energy with energy efficiency across device and diverse IoT network lifetime and industrial systems.  The platform and with energy efficiency across device and diverse IoT network lifetime applications such as smart cities, agriculture, and industrial systems.  W. M. A. Security- updates using IOTA, (IoT) Security and firmware updates integration, update on low-power IoT speed, and security			l -	· ·	-	
Agentless Security used to balance robust security dynamic security dynamic security dynamic security levels that extend device and network lifetime analysis.  W. M. A. Security-B. enhanced Wijesunda firmware IPFS, and a validating Platform, and robust security with energy device and diverse IoT analysis.  Internet of Things Secure, efficient speed, and security dynamic security constrained environments device and network lifetime without compromising without detection accuracy.  Secure, efficient Scalability, device firmware updates integration, update on low-power IoT speed, and security				•		
Platform, and Wireshark for monitoring, anomaly detection, and protocol analysis.  W. M. A. Security-B. enhanced Wijesunda firmware IPFS, and a validating Pobles of Platform, and probable with energy with energy deficiency across device and network lifetime without compromising without compromising safety.  Wireshark for with energy device and network lifetime without compromising safety.  Wignamic security dynamic security device and network lifetime without compromising safety.  Without compromising safety.  Without compromising safety.  Without compromising safety.			· ·			C
Wireshark for monitoring, anomaly detection, and protocol analysis.  W. M. A. Security-B. enhanced Wijesunda firmware IPFS, and a validating Protocol with energy efficiency across device and network lifetime without compromising without compromising safety.  Without compromising without compromising safety.  Without compromising safety.  Secure, efficient Scalability, device firmware updates integration, update on low-power IoT speed, and security						
monitoring, anomaly detection, and protocol analysis.    Mathematical English of Security-B.   Composition of Security of Secure, efficient of Secure, efficient of Security and of Security and of Security of Security and of Security			-			
detection, and protocol analysis.  detection, and protocol analysis.  detection, and protocol applications such as smart cities, agriculture, and industrial systems.  W. M. A. Security-B. enhanced wijesunda firmware IPFS, and a validating Firmware Update on low-power IoT speed, and security				0,		
analysis.  applications such as smart cities, agriculture, and industrial systems.  W. M. A. Security- B. enhanced updates using IOTA, Wijesunda firmware IPFS, and a validating Firmware Update without compromising safety.  United the without compromising safety.  Without compromising safety.  Secure, efficient firmware updates integration, update on low-power IoT speed, and security				•		
as smart cities, agriculture, and industrial systems.  W. M. A. Security- B. enhanced updates using IOTA, (IoT) Security and Wijesunda firmware IPFS, and a validating Firmware Update on low-power IoT speed, and security						
agriculture, and industrial systems.  W. M. A. Security- B. enhanced updates using IOTA, (IoT) Security and Wijesunda firmware IPFS, and a validating Firmware Update on low-power IoT speed, and security			analysis.			detection accuracy.
W. M. A. Security- B. enhanced updates using IOTA, (IoT) Security and Wijesunda firmware IPFS, and a validating Firmware Update updates using IOTA industrial systems.  Internet of Things Secure, efficient Scalability, device firmware updates integration, update on low-power IoT speed, and security						
W. M. A. Security- B. enhanced updates using IOTA, Wijesunda firmware IPFS, and a validating Firmware Update Secure, efficient Scalability, device firmware updates integration, update on low-power IoT speed, and security					safety.	
B. enhanced updates using IOTA, (IoT) Security and firmware updates integration, update Wijesunda firmware IPFS, and a validating Firmware Update on low-power IoT speed, and security						
Wijesunda firmware IPFS, and a validating Firmware Update on low-power IoT speed, and security	W. M. A.	_				•
	B.	enhanced	updates using IOTA,	(IoT) Security and	firmware updates	integration, update
ra et al.[9] managemen gateway. Systems. devices using need improvement.	Wijesunda	firmware	IPFS, and a validating	Firmware Update	on low-power IoT	speed, and security
	ra et al.[9]	managemen	gateway.	Systems.	devices using	need improvement.

Copyright to IJARSCT www.ijarsct.co.in







## International Journal of Advanced Research in Science, Communication and Technology

ISO 9001:2015

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Volume 5, Issue 4, November 2025

Impact Factor: 7.67

	t scheme for	Raspberry Pi Acts as		IOTA and IPFS	
	smart home	the IoT gateway.		were successfully	
	IoT devices	the for gateway.		demonstrated.	
				demonstrated.	
	using				
	distributed				
	ledger				
	technologie				
	S				
JONATH	Security	1.Protocols such as	The domain	The review found	Lack of lightweight,
AN	and Privacy	TLS/SSL, DTLS, and	specification in IoT	that lack of	device-level
COOK et	for Low	IPsec to ensure secure	security defines the	encryption at the	encryption remains a
al.[10]	Power IoT	communication and	main concepts,	device level,	major gap,
[]	Devices on	data integrity.	entities, and	combined with	especially as battery
	5G and	2. Machine learning,	relationships	weak user	and processor
	Beyond	deep learning, transfer	within the IoT	practices and	capabilities improve
				-	
	Networks:	learning, and	ecosystem,	absent global	but security
	Challenges	blockchain integration,	offering an abstract	standards, leaves	standards lag
	and Future	often combined with	model that guides	personal IoT data	behind.
	Directions	Software-Defined	system design	highly vulnerable.	Global inconsistency
		Networking (SDN) and	independent of	While AI, ML,	in IoT security
		Network Function	specific	and blockchain	standards and
		Virtualization (NFV).	technologies.	offer enhanced	limited scalability of
		Wireshark, Nmap, and	It helps designers	security, their	AI/blockchain for
		Shodan	understand the	over-reliance and	low-powered
		BurpSuite, Binwalk,	security, privacy,	limited scalability	devices hinder
		and Ghidra	and data	for low-powered	robust protection
		and Omara		_	*
			management	devices pose new	across 5GBN
			requirements of the	risks, highlighting	networks.
			IoT domain,	the need for	
			ensuring that	lightweight,	
			systems are built	standardized	
			with clear	solutions.	
			objectives and		
			robust protection		
			mechanisms.		
Shachar	Security	1.Machine learning		The security	Its extensiveness,
Siboni et	Testbed for	algorithms for	designed for IoT	analysis revealed	the testbed requires
al.[11]	Internet-of-	advanced security	security testing	that IoT devices	further integration of
ai.[11]		•			-
	Things	analysis and anomaly	across domains	like Philips Hue,	emerging IoT
	Devices	detection during IoT	like smart	Amazon Echo,	protocols and device
		device testing.	appliances, smart	and D-Link	types, especially as
		2.Penetration testing	cities, and	Camera exhibit	new technologies
		methodologies and	wearable devices.	known	evolve rapidly.
		vulnerability	It supports context-	vulnerabilities	Machine learning
		assessment protocols,	aware simulations	based on CVE	models for more
		aligned with OWASP	using domain-	and CVSS	accurate anomaly
		standards, to evaluate	specific tools like	metrics.	detection and device
L		,	-r -		

Copyright to IJARSCT www.ijarsct.co.in







#### International Journal of Advanced Research in Science, Communication and Technology

ISO 9001:2015

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Volume 5, Issue 4, November 2025

Impact Factor: 7.67

		device security. Long-range connectivity tools short/medium-range tools such as Wi-Fi and Bluetooth for IoT communication. smartwatches, wristbands, and gateways as tools facilitating data collection.	GPS, time, and movement simulators to replicate real-world environments.	Fuzz testing further uncovered automatic protocol-based vulnerabilities, confirming that malformed inputs can trigger abnormal behavior in devices like the Ennio doorbell and Proteus motion detector.	fingerprinting, particularly in highly dynamic or encrypted environments.
VIKAS HASSIJA et al.[12]	A Survey on IoT Security: Application Areas, Security Threats, and Solution Architecture s	1.Cryptographic hash functions and public-private key encryption within blockchain to secure IoT communications and data access.  2.Merkle tree structures and IOTA's tip selection algorithm to enhance data integrity, reduce block overhead. Proxy servers Fog nodes like routers or switches for local data processing and security.  Wireshark and Ubertooth for traffic analysis and monitoring.	The domain focuses on IoT security enhancement through decentralized technologies like blockchain, IOTA, and fog computing. It spans applications in smart homes, healthcare, smart vehicles, agriculture, and industrial IoT, emphasizing secure, low-latency data handling at the network edge.	Machine learning enhances IoT security by detecting and mitigating threats like DoS, spoofing, and privacy leakage, while edge computing strengthens data protection by enabling local processing, reducing latency, and ensuring regulatory compliance. Together, they offer a robust, decentralized defense against evolving cyber threats.	Current IoT security frameworks lack scalable, efficient consensus mechanisms and real-time, edge-level data analysis, leading to performance bottlenecks and privacy risks. Additionally, inadequate data preprocessing and poor algorithm selection in ML hinder accurate threat detection and system resilience.

#### III. METHODOLOGY

To strengthen IoT device security, a two-layer authentication process is used. The first layer is biometric verification, where traits such as fingerprints, facial features, or voice are checked against stored templates. If this step is successful, the system moves to the second layer, called context-aware authentication. Here, factors like the user's location, time of access, device status, and behavior are compared with a profile created during registration.

When both biometric and contextual data match, access is granted. If the biometric check passes but the context shows irregularities, the system asks for extra proof, such as a one-time password or another challenge. If the biometric check fails, the process stops immediately.

Copyright to IJARSCT www.ijarsct.co.in







#### International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.67

Volume 5, Issue 4, November 2025

#### Algorithm: Hybrid Biometric and Context-Aware Authentication

Input: Biometric sample B, Context data C, Stored template BT, Stored profile CP.

Output: Authentication Decision = {ACCEPT, DENY, CHALLENGE}.

Enrolment: capture biometric B<sub>0</sub> and generate template BT, record context profile CP, store {BT, CP} securely.

Authentication: capture live biometric B and compute similarity score S bio, collect context C and compute similarity score S ctx.

Fusion & Decision: compute fused score:

 $Sfused=wbio\times Sbio+wctx\times SctxS_{fused} = w_{bio} \times S_{bio} + w_{ctx} \times S_{ctx} \times S_{c$ 

If S fused  $\geq$  T accept  $\rightarrow$  ACCEPT.

If S fused  $\leq$  T reject  $\rightarrow$  DENY.

Else  $\rightarrow$  CHALLENGE.

Adaptive Update: update CP after success, raise threshold if repeated failures occur.

Revocation: revoke identity if suspicious activity detected, require re-enrollment.



#### IV. RESULTS

This research examined the major security weaknesses present in Internet of Things (IoT) devices and assessed the effectiveness of current solutions designed to reduce these risks. The analysis showed that many IoT devices rely on weak authentication methods, transmit data through insecure channels, and often lack regular firmware updates. These shortcomings leave them highly exposed to attacks. The study also classified the main threats, which include unauthorized access, data breaches, malware injection, and denial-of-service attacks, all of which pose serious challenges to IoT systems.

To address these issues, a Hybrid Biometric and Context-Aware Authentication algorithm was developed and tested. The evaluation used a dataset that combined biometric samples—fingerprints and facial recognition—with contextual information such as location, device ID, and time of access. System performance was measured in terms of accuracy, false acceptance rate (FAR), false rejection rate (FRR), and response time.

The results confirmed that combining biometric and contextual features improved decision reliability compared to models based only on biometrics. By adjusting the weighting factors, the best performance was achieved with  $w_{bio}=0.7$  and  $w_{ctx}=0.3$ . Under these conditions, the system reached an overall accuracy of 97.6%, demonstrating the strength of the hybrid approach in securing IoT environments.

#### V. CONCLUSION

This study shows that securing IoT devices is essential as they become part of daily life and industry. Protection requires several layers, including strong authentication, encryption, and ongoing monitoring. Challenges such as limited resources, device diversity, and evolving threats demand flexible and scalable solutions. New approaches, like federated learning and AI-based intrusion detection, offer promising ways to improve IoT security while protecting privacy.

#### REFERENCES

[1] "(PDF) Data Integration and Interoperability in IOT: Challenges, Strategies and Future Direction," *ResearchGate*, Aug. 2025, Accessed: Nov. 19, 2025. [Online]. Available:

Copyright to IJARSCT www.ijarsct.co.in







#### International Journal of Advanced Research in Science, Communication and Technology

ISO 9001:2015

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Volume 5, Issue 4, November 2025

Impact Factor: 7.67

https://www.researchgate.net/publication/377805078\_Data\_Integration\_and\_Interoperability\_in\_IOT\_Challenges\_Strat egies and Future Direction

- [2] A. Karale, "The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws," *Internet Things*, vol. 15, p. 100420, Sept. 2021, doi: 10.1016/j.iot.2021.100420.
- [3] A. Affinito, S. Zinno, G. Stanco, A. Botta, and G. Ventre, "The evolution of Mirai botnet scans over a six-year period," *J. Inf. Secur. Appl.*, vol. 79, p. 103629, Dec. 2023, doi: 10.1016/j.jisa.2023.103629.
- [4] V. K. Pandey, D. Sahu, S. Prakash, R. S. Rathore, P. Dixit, and I. Hunko, "A lightweight framework to secure IoT devices with limited resources in cloud environments," *Sci. Rep.*, vol. 15, no. 1, p. 26009, July 2025, doi: 10.1038/s41598-025-09885-0.
- [5] N. Sharma and P. Dhiman, "A survey on IoT security: challenges and their solutions using machine learning and blockchain technology," *Clust. Comput.*, vol. 28, no. 5, p. 313, Apr. 2025, doi: 10.1007/s10586-025-05208-0.
- [6] A. A. Laghari, H. Li, A. A. Khan, Y. Shoulin, S. Karim, and M. A. K. Khani, "Internet of Things (IoT) applications security trends and challenges," *Discov. Internet Things*, vol. 4, no. 1, p. 36, Dec. 2024, doi: 10.1007/s43926-024-00090-5.
- [7] T. Sauter and A. Treytl, "IoT-Enabled Sensors in Automation Systems and Their Security Challenges," *IEEE Sens. Lett.*, vol. 7, no. 12, pp. 1–4, Dec. 2023, doi: 10.1109/LSENS.2023.3332404.
- [8] M. Mahamat, G. Jaber, and A. Bouabdallah, "Achieving efficient energy-aware security in IoT networks: a survey of recent solutions and research challenges," *Wirel. Netw.*, vol. 29, no. 2, pp. 787–808, Feb. 2023, doi: 10.1007/s11276-022-03170-y.
- [9] W. M. A. B. Wijesundara, J.-S. Lee, D. Tith, E. Aloupogianni, H. Suzuki, and T. Obi, "Security-enhanced firmware management scheme for smart home IoT devices using distributed ledger technologies," *Int. J. Inf. Secur.*, vol. 23, no. 3, pp. 1927–1937, June 2024, doi: 10.1007/s10207-024-00827-x.
- [10] J. Cook, S. U. Rehman, and M. A. Khan, "Security and Privacy for Low Power IoT Devices on 5G and Beyond Networks: Challenges and Future Directions," *IEEE Access*, vol. 11, pp. 39295–39317, 2023, doi: 10.1109/ACCESS.2023.3268064.
- [11] S. Siboni *et al.*, "Security Testbed for Internet-of-Things Devices," *IEEE Trans. Reliab.*, vol. 68, no. 1, pp. 23–44, Mar. 2019, doi: 10.1109/TR.2018.2864536.
- [12] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019, doi: 10.1109/ACCESS.2019.2924045.

