Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606

Volume 07 Issue 01
2024

Research Article
https://doi.org/10.56979/701/2024

Techniques for Authentication and Defense Strategies to Mitigate IoT Security Risks

Ayesha Munir[1*], Irshad Ahmed Sumra[1], Rania Naveed[1], and Muhammad Aaqib Javed[2]

[1]Department of Information Technology, Lahore Garrison University, Lahore, 54000, Pakistan.
[2]Department of Computer Science, University of Alabama at Birmingham, Birmingham, USA.
Corresponding Author: Ayesha Munir. Email: munirayesha776@gmail.com

Received: November 11, 2023 **Accepted:** March 29, 2024 **Published:** June 01, 2024

Abstract: Internet of Things (IoT) has rapidly evolved into a transformative technology, impacting various facts of daily life and industry. However, its widespread adoption has been impeded by significant challenges, particularly in the realms of security, privacy, interoperability, scalability, and Quality of Service (QoS). These challenges represent critical obstacles that must be addressed to ensure the reliability and efficacy of IoT systems. It addresses security vulnerabilities through multi-layered measures including encryption, authentication mechanisms, anomaly detection, and secure firmware updates, while also prioritizing privacy preservation through privacy-by-design principles and data anonymization techniques. Additionally, methodology advocates for interoperability frameworks, scalability strategies encompassing cloud-based architectures and edge computing paradigms, and Quality of Service enhancements through performance monitoring and adaptive resource allocation. By implementing these methodologies, we aim to overcome the fundamental challenges facing IoT deployment and pave the way for a more secure, interoperable, scalable, and reliable IoT ecosystem, underscoring the importance of comprehensive solutions to unlock the full potential of the Internet of Things.

Keywords: IOT; Data Security; (Wireless Sensor Network) WSN; Communications Protocols; (One-Time Password Authentication) OTP; (Elliptic Curve Cryptography) ECC; (Quality of Service) QOS.

1. Introduction

Smoother communication between IoT devices is made possible by advancements in mobile communication, RFID, Wireless Sensor Networks (WSN), and cloud computing. To communicate and send crucial data to a central system, these devices—which include cellphones, laptops, PDAs, tablets, and other handheld embedded devices—make use of affordable sensors and Wireless Communication Systems (WCS)[1]. This data is processed by the central system, which also routes it to the proper locations. As internet and communication technology advance, our lives are increasingly focused on virtual environments. Individuals can now live in the real world and work, shop, and communicate in virtual worlds supplied via networks [2]. The difficulty of fully automating all human actions is presented by this integration. The Internet of Things (IoT) has effectively bridged the virtual and real worlds on a single platform. The primary goals of IoT include creating smart environments, self-aware independent devices, intelligent living, smart items, intelligent healthcare, and smart cities [3].

With more and more devices connected to the internet, the adoption rate of IoT devices is very high. By 2020, 200 million connections across 30 million linked devices were expected to bring in 700 million euros in income. By 2020, there will be 24 million IoT devices in China, up from an estimated 9 million at the beginning of the year. IoT is expected to change lives, business models, and lifestyles in the future [4] [5].

A modern technology known as the Internet of Things (IoT) makes it easier to build networks that link different virtual and real-world objects. Foundational components of the Internet's early growth included file sharing, email, the World Wide Web, and client-server architecture. A modest computer network that connected personal computers at first has grown into a massive network that connects billions of smart gadgets inside intricate systems. Sensors and actuators intended to observe, regulate, and communicate with their physical environment power these systems [6] [7].

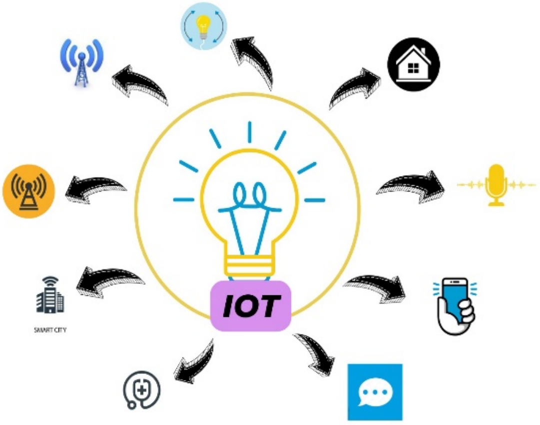

Figure 1. Positive Impact of IOT

In the process of developing robotics, networked systems, the Internet of Things was created. Real-time operational information is provided by a huge amount of data that is gathered from various manufacturing process phases using IoT-enabled sensors and devices [3].

IoT has many benefits, but it also has three main drawbacks: data collecting, data transmission, and data security. Numerous protocols have been established to enable the transfer of acquired data, enabling IoT devices to connect to existing networks and share information. A variety of sensing instruments have been developed and adapted to assist data collecting for IoT devices. But frequently, data security does not get the attention it needs. As a result, IoT is susceptible to both established and new security risks, such as worries about authorization, data security, and authentication.

Authentication vulnerabilities can lead to various attacks, such as replay attacks, Denning–Sacco attacks, denial-of-service attacks, and password guessing attacks. Additionally, authenticating IoT devices across heterogeneous and interconnected protocols poses a significant challenge. These protocols must also address the limitations of IoT devices, such as energy consumption, limited memory size, and low processing capability. Although there is no standard consensus on IoT architecture, the three-layer technology model is widely accepted, as illustrated in Figure 2.

1.1. Cognitive layer of a three-layer IOT Architecture

The physical layer of the Internet of Things architecture is this cognitive layer. Typically, embedded systems and sensors are used in these applications. As needed, they gather a lot of data. This include edge devices, environmental sensors, and actuators as well. It identifies objects and other smart things around you in addition to particular geographic features. The appropriate control operations on the execution device are likewise carried out using control information from the network layer [27] [43].

1.2. Network layer of a three-layer IOT Architecture

The information collected by these devices must be distributed and stored. The network layer is responsible for this. Connect intelligent things with other intelligent or smart objects. It is also responsible for data transfer. The network layer connects intelligent elements, network devices, and servers. It is also used for distributing and analyzing sensor data. It is important to note that network layer data transfer functionality includes both local and remote data transfer. Long-distance data transmission takes place via the Internet, which consists of a number of dedicated networks, mobile networks, satellite networks, etc.

1.3. Application layer of a three-layer IOT Architecture

The user and application layer are connected. In charge of giving customers access to software resources. For instance, a smart home app enables users to initiate a coffee maker by merely tapping a button within the app. Customers can access application-specific resources from this layer. Defines a number of Internet of Things applications, including expert systems, databases, cloud computing, smart homes, middleware, data mining, and smart cities and health. It is still required to be aware of intelligent Internet of Things applications and information technologies.

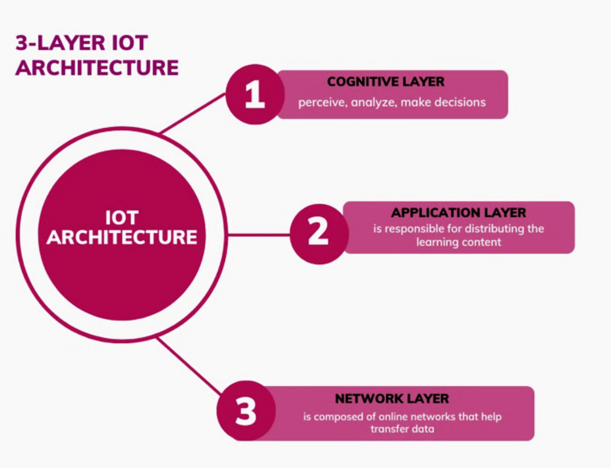
3-LAYER IOT ARCHITECTURE
IOT ARCHITECTURE
1
COGNITIVE LAYER
perceive, analyze, make decisions
2
APPLICATION LAYER
is responsible for distributing the learning content
3
NETWORK LAYER
is composed of online networks that help transfer data

Figure 2. Three Layer IOT Architecture.

It will be divided into the following sections: Section 2 defines the IOT architecture. Section 3 describes the challenges facing in IOT. it describes the security and privacy issues, interoperability/standards issues, ethics, law and regulatory rights, scalability, availability and reliability, QOS (Quality of services). Section 4 discusses the analysis of different types of attacks and possible solutions. Section 5 discusses IOT Authentication Techniques. Finally, in Section 6, the conclusion is presented, as well as recommendations for future workThis paper is organized as follows.

2. IoT Challenges

As IOT-based systems are involved in every aspect of human life and different technologies are involved in transferring data between embedded devices, the problem becomes complex and poses several issues and challenges. Therefore, IoT developers need to think about new problems and provide solutions. The Internet of Things (IoT) offers numerous benefits, but it also presents several significant challenges that need to be addressed to ensure its effective and secure implementation. Here are some of the primary challenges associated with IoT:

2.1. Security and Privacy Issues

Security and privacy pose significant and intricate challenges in the IoT domain, driven by a plethora of threats, cybersecurity incidents, risks, and vulnerabilities. Challenges such as inadequate authorization and authentication, vulnerable software and firmware, insecure web interfaces, and insufficient encryption at the transport layer exacerbate concerns regarding data security at the device level. To mitigate security risks and cyber threats, robust security measures need to be embedded throughout all layers of the IoT architecture. Various protocols have been devised and deployed at different communication levels to enhance the security and privacy of IoT systems effectively [32].

Popular cryptographic protocols such as “Secure Socket Layer (SSL)” and “Datagram Transport Layer Security (DTLS)” are widely employed to implement certificate-based authentication and symmetric encryption for safeguarding data transmitted over untrusted networks. These protocols are typically situated between the transport layer and the application layer, providing security measures for a variety of IoT systems. However, certain IoT applications might necessitate different approaches for securing communication between IoT devices. The utilization of wireless technology in IoT system communications increases susceptibility to security threats, highlighting the need for strategies to detect malicious behavior and facilitate self-repair or recovery procedures [38].

Privacy emerges as another critical concern essential for fostering trust in IoT systems. Users must feel safe and assured in their interactions with IoT solutions. Thus, maintaining robust authorization and authentication procedures on secure networks is imperative to establish communication between trusted entities. An additional challenge lies in the differing privacy policies of various communicating objects within an IoT system. Consequently, each object must be capable of verifying the privacy policies of others in the system before sharing data [35].

2.2. Interoperability/ Standards Issues

Interoperability concerns the ability of varied IoT devices and systems to exchange information irrespective of their software and hardware specifications. Challenges in achieving interoperability often stem from the diverse technologies and solutions employed in IoT development. The concept encompasses four key levels - technical, semantic, syntactic, and organizational. In diverse IoT environments, systems incorporate multiple features to enhance interoperability, facilitating seamless communication between different objects. Additionally, merging different IoT platforms by their functionalities allows for a diverse range of solutions for IoT users. Researchers have underscored the importance of interoperability and have introduced several solutions, labeled as interoperability management approaches. These solutions include adapters/gateways, virtual networks/overlays, and service-oriented architectures.

2.3. Ethics, Law and Regulatory Rights

The rapid growth and adoption of IoT technologies have introduced numerous ethical, legal, and regulatory challenges that need addressing to ensure responsible usage and protection of users' rights. Ethical concerns include privacy issues, data ownership, surveillance, and algorithmic bias, requiring transparent data collection, clear data ownership policies, and fair algorithms. Legally, IoT systems must comply with data protection laws like GDPR, establish clear liability frameworks, and protect intellectual property. Regulatory challenges involve the lack of standardization, the need for robust security regulations, consumer protection, and managing cross-border data transfers. To tackle these issues, IoT developers should integrate ethical considerations into system design, ensure legal compliance, participate in standardization efforts, educate consumers on security and privacy, and collaborate with stakeholders to develop best practices and regulatory frameworks. By doing so, the IoT industry can build trust, ensure compliance, and promote a sustainable and responsible IoT ecosystem.

2.4. Scalability, Availability and Reliability

Scalability, availability, and reliability are crucial for the effective deployment and operation of IoT systems. Scalability ensures that an IoT system can handle an increasing number of devices, services, and data volumes without performance degradation, exemplified by cloud-based IoT systems that support expansion by adding new devices and resources as needed. Availability guarantees that IoT resources and services are accessible at all times, regardless of location, which is vital in distributed environments where multiple small-scale IoT networks connect to a global platform. Reliability ensures consistent and dependable performance, even in the face of network disruptions or varying device capabilities. Achieving these factors requires addressing challenges such as managing diverse device requirements, developing robust frameworks, and implementing independent and reliable data transmission channels to prevent service interruptions.

2.5. Quality of Service (QoS)

Quality of Service (QoS) is essential for evaluating and ensuring the performance, efficiency, and reliability of IoT devices, systems, and architectures. Key QoS metrics for IoT applications include reliability, cost, energy consumption, security, availability, and service time. A robust IoT ecosystem must adhere to these standards to meet user expectations and application requirements. To ensure reliability, QoS metrics must be clearly defined and tailored to specific use cases. Various approaches, as detailed by researchers like White et al., can be used for QoS evaluation, acknowledging trade-offs between different quality factors. High-quality models are crucial to manage these trade-offs effectively, offering a comprehensive range of quality factors suitable for evaluating IoT services. Additionally, IoT services must address security concerns, user privacy, and the unique challenges posed by the diversity of devices and networks involved. By focusing on QoS, IoT systems can deliver consistent, reliable, and efficient performance, thereby enhancing user trust and satisfaction. User privacy can be compromised in various ways, posing significant security threats in IoT environments. Some of these security threats include:

2.5.1. E2E data lifecycle protection

End-to-End data protection is provided across the complete network to ensure data security in IoT environments. Data is collected from various interconnected devices and instantly shared with other devices. Therefore, a framework for data protection, data confidentiality, and data protection controls across the data lifecycle is required as discusses in Figure 03.

2.5.2. Secure Planning

Connectivity and communication between IoT devices are context-dependent, requiring a consistent level of security. For instance, if local devices and sensors within a home network communicate securely, the same security policies must apply to interactions with external devices.

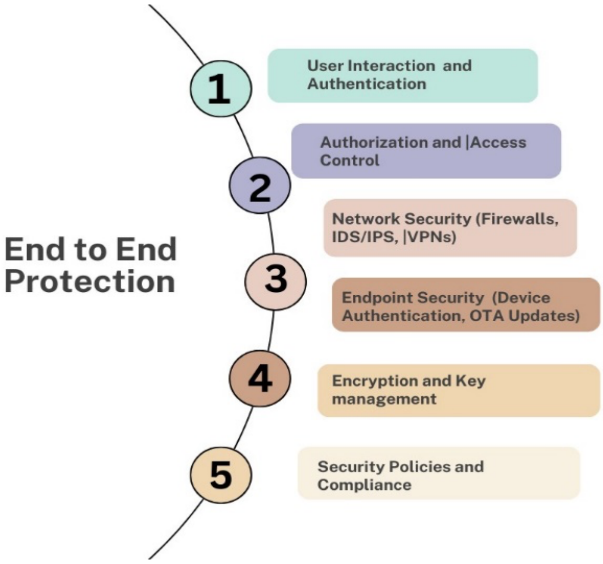
End to End Protection
1
User Interaction and Authentication
2
Authorization and |Access Control
3
Network Security (Firewalls, IDS/IPS, |VPNs)
Endpoint Security (Device Authentication, OTA Updates)
4
Encryption and Key management
5
Security Policies and Compliance

Figure 3. E2E Life Cycle

2.5.3. Usable Security and privacy

Most security and privacy issues stem from user misconfiguration. Implementing such privacy policies and complex security mechanisms is often very challenging and impractical for users. Therefore, users might need to choose a security and privacy policy that can be automatically applied.

Table 1. Comparative Analysis

Source	Focus	Perspective	Time	Novelty
[26]	IoT Information Processing	Low-Latency Processing in "C-NAT" IoT Platform	2023	Emphasis on Low-Latency Processing for IoT Information in the "C-NAT" Platform.
[28]	Attack Detection in IoT Environment	Enhanced Attack Detection and Explanation	2023	Improved Intrusion Detection System for IoT Environments with a Focus on Enhanced Attack Detection and Explanation.
[29]	Blockchain-Based IoT Payment	Payment and Marketplaces in IoT	2022	Survey on Blockchain-Based IoT Payment and Marketplaces, Providing Insights into Current Trends and Challenges
[30]	Intelligent IoT Environments	Performance-Energy Tradeoffs	2022	Exploration of Learning, Computing, and Trustworthiness in Intelligent IoT Environments with a Focus on Performance-Energy Tradeoffs
[21]	Secure and lightweight authentication scheme for IoT infrastructure	Security solution for IoT	2021	Proposes a secure and lightweight authentication scheme for the next-gen IoT infrastructure.
[5]	Internet of Things: Ecosystem	Quantitative insights into IoT growth	2020	Offers quantitative data on the IoT ecosystem, highlighting device growth.

	and device statistics			
[6]	Internet of Things (IoT): Definition, characteristics, etc.	IoT definition and characteristics	2016	Explores the definition, characteristics, and challenges of IoT.
[1]	Security and privacy issues in IoT	Survey on IoT	2014	In-depth exploration of security and privacy challenges in the IoT.
[2]	Security and privacy in the Internet of Things	Current status and open issues	2014	Identification of current status and open issues in IoT security and privacy.
[3]	Vision of IoT: Applications, challenges, and opportunities	China perspective	2014	Provides a vision of IoT with a focus on applications, challenges, and China's perspective.

3. Methodology

IoT is susceptible to various types of attacks, including active and passive attacks, which can easily affect functionality and negate the benefits of the service. In a passive attack, the intruder simply tracks the node or sometimes steals information, but does not physically attack it. However, aggressive attacks physically disrupt performance.

These active attacks are further classified into two categories: internal attacks and external attacks. These vulnerable attacks can prevent devices from intelligently communicating. Therefore, security restrictions must be applied to protect your device from malicious attacks. This section describes the different types of attacks, the nature/behavior of the attacks, and the threat level of the attacks.

$$R= p_{detection}*p_{success}*S$$

where:

- R is the overall risk.
- $p_{detection}$ is the probability of detecting the attack.
- $p_{success}$ is the probability of the attack being successful.
- S is the severity of the attack

Attack levels are classified into four types according to their behavior and possible solutions to the threats/attacks are suggested.

3.1. Low Level Attack

Low-level attacks in IoT target the fundamental layers of devices and networks by exploiting vulnerabilities in hardware, firmware, and basic communication protocols. These attacks include physical tampering to modify device components or extract data, side-channel attacks exploiting emissions like electromagnetic leaks or power consumption patterns, and firmware attacks such as firmware injection and exploitation to alter device operation or gain unauthorized access. Additionally, radio frequency (RF) attacks, including jamming, which disrupts wireless communications with noise, and replay attacks, which capture and retransmit legitimate signals to trick devices, pose significant threats. These low-level attacks can severely compromise the security and functionality of IoT systems, highlighting the need for robust protective measures.

3.2. Medium Level Attack

Medium-level attacks in IoT focus on the network and protocol layers, exploiting vulnerabilities in communication protocols, network configurations, and software applications. These attacks include Man-in-the-Middle (MitM) attacks, where an attacker intercepts and potentially alters communication between devices, and Denial-of-Service (DoS) attacks, which overwhelm network resources to disrupt service. Protocol exploitation, such as weaknesses in MQTT or CoAP, can also be targeted to gain unauthorized access or manipulate data. Additionally, attacks like packet sniffing can capture sensitive information transmitted over the network, while insecure API exploitation can lead to unauthorized control or data breaches. These medium-level attacks can severely impact the reliability and security of IoT systems, necessitating robust network security measures and secure communication protocols.

3.3. High Level Attack

Attacks which are high leveled in severity escalation, compromising the intellectual property. These kind of attacks are involved manipulate the data, malicious activities like "multi-factor" and "digital signature" type authentication must be used to verification the integrity. Intrusion prevention system (IPS) and end point protection solutions can also detect and prevent unauthorized modifications to IoT systems. When an attack occurs on the network, compromising data integrity or changing data [44].

3.4. Severe Attack

Severe attacks on IoT systems target the overall integrity, availability, and security of the entire network, often causing widespread disruption and significant damage. These include Distributed Denial-of-Service (DDoS) attacks, where multiple compromised devices flood the network with traffic, overwhelming servers and rendering services unavailable. Advanced Persistent Threats (APTs) involve prolonged and targeted cyberattacks where attackers infiltrate the network, maintain undetected access, and exfiltrate sensitive data over time. Ransomware attacks can encrypt critical data and systems, demanding payment for restoration. Botnet attacks leverage a network of infected IoT devices to launch coordinated cyberattacks, further exacerbating the impact. These severe attacks can cripple IoT networks, compromise vast amounts of data, and cause substantial financial and operational damage, highlighting the need for comprehensive security strategies and defenses [41] [45].

3.5. IOT Authentication Techniques

Since IOT has access to all user's information, user privacy must be protected from malicious attacks. Also do not allow unauthorized persons to access your device. Therefore, you must verify the user's identity before granting authorization. Therefore, the user's identity can be verified in various ways [46].

However, the most commonly used are authentication systems based on prior sharing of secrets, keys or passwords. Therefore, this section describes the techniques used to strengthen authentication in IOT Environments.

3.5.1. One Time password Authentication

A one-time password (OTP), also known as a dynamic password, is a password that is useful for authenticating in transactions. A literature review has proposed various OTP authentication protocols to secure communications in IoT environments. These protocols are based on various mechanisms such as time synchronization, hash parts (MD5, SHA1, SHA256), and RSA encryption. Furthermore, they are all based on Knapsack OTP Problem. Here's a simplified implementation:

	0	1	2	3	4	5	6	7	8	9	10	11	12
0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	×	×	5	5	5	5	5	5	5	5	5	5	5
2	×	×	×	8	8	13	13	13	13	13	13	13	13
3	×	×	×	×	×	×	2	2	7	10	10	10	10
4	×	×	×	×	×	×	×	9	9	14	17	17	17
5	×	×	×	×	×	×	×	×	7	7	12	15	15

Secret Key: [5, 8, 2, 9, 7]
Weights: [2, 3, 6, 7, 8]
N = 5
W = 12

Now, for a user with a unique identifier (e.g., user ID), you derive a key by combining the secret key and the user-specific information.

Let's say the derived key is [3, 5, 2, 4, 6]. Now, you apply the knapsack algorithm to generate the OTP:

Table 2. OTP

pi	wi
5	2
8	3
2	6
9	7
7	8

Using knapsack formula,

V[i,w]=max[v(i-1),wi], v[(i-1),w-wi]+Pi

OTP Generation:

Digit 1: Select weight 6 (from the weights) because the derived key has a corresponding 1 at the first position.

Digit 2: Select weight 8.

Digit 3: Select weight 3.

Digit 4: Select weight 7.

Digit 5: Select weight 7.

The generated OTP, based on this example, is 63877.

Time complexity of this problem is O (n).

3.5.2. ECC-based Mutual Authentication

ECC-based mutual authentication is a cryptographic method that uses Elliptic Curve Cryptography (ECC) to securely verify the identities of both communicating parties in IoT systems. This approach leverages ECC's efficiency, providing strong security with smaller key sizes, which is ideal for resource-constrained IoT devices. In this process, each device generates a pair of keys (private and public) and exchanges public keys. Using the exchanged public keys and their own private keys, devices independently generate a shared secret, which is then used to encrypt and decrypt authentication challenges. By verifying these challenges, both devices confirm each other's identities, ensuring secure communication. ECC-based mutual authentication offers robust protection against various attacks, such as replay and man-in-the-middle attacks, while maintaining low computational and energy overhead, making it particularly suitable for the IoT environment.

3.5.3. ID and Password Based Authentication

ID and password-based authentication is one of the most common and straightforward methods used to verify a user's identity. This method requires users to provide a unique identifier (ID) and a corresponding password to gain access to a system or resource. It follows according rules:

- First, how is user data stored on the server?
  Can the server protect the user from theft verifier attacks or insider attacks?
- Second, can the user forget authentication parameters?

There is a possibility that the Therefore, the following authentication cannot be performed.

In this case, it is not appropriate to store personal IDs on electronic devices (laptops, tablets, smartphones), even if they are not connected to a public network. Third, transmitting user IDs over public networks presents additional challenges, so using a hash function or cryptographic algorithm is recommended.

3.5.4. Certificate Based Authentication

Certificate-based authentication is a method of confirming the identity of a communicating device or user within a network environment. This process involves the use of digital certificates to validate the credentials of parties involved in data exchanges.

3.5.5. Blockchain Technology

Certificate-based authentication is a method of confirming the identity of a communicating device or user within a network environment. This process involves the use of digital certificates to validate the credentials of parties involved in data exchanges.

4. Conclusion and Future Work

The Internet of Things (IoT) has experienced substantial growth, integrating various real-world and virtual components through technologies like Wireless Sensor Networks (WSN), RFID, and cloud computing. With predictions of over 38 billion connected devices by 2025, IoT has revolutionized fields such as social security, agriculture, and smart grids. The three-layer IoT architecture, which includes the cognitive, network, and application layers, is essential for data collection, processing, and delivery. However, IoT faces significant challenges including data security, interoperability, ethical considerations, and scalability. Security issues, particularly authentication vulnerabilities, underscore the need for robust protective measures. To address these concerns, several authentication methods are employed, including one-time passwords, ECC-based mutual authentication, ID and password-based authentication, certificate-based authentication, and blockchain technology. Despite these advancements, IoT remains vulnerable to various attacks, highlighting the necessity of implementing effective security measures. In conclusion, while IoT offers tremendous potential, it is crucial to tackle security challenges, ensure interoperability, and address ethical considerations to sustain its growth and impact. Future research could enhance IoT security further, and there is room to improve classification methods and introduce additional functions to handle specific errors.

References

1. J. S. Kumar and D. R. Patel, “A survey on internet of things: Security and privacy issues,” International Journal of Computer Applications, vol. 90, no. 11, 2014.
2. M. Abomhara and G. M. Køien, “Security and privacy in the internet of things: Current status and open issues,” in Privacy and Security in Mobile Systems (PRISMS), International Conference on. IEEE, 2014, pp. 1–8.
3. S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, “A vision of iot: Applications, challenges, and opportunities with china perspective,” IEEE Internet of Things journal, vol. 1, no. 4, pp. 349–359, 2014.
4. L. Atzori, A. Iera, and G. Morabito, “The internet of things: A survey,” Computer. Network., vol. 54, no. 15, pp. 2787–2805, Oct 2010.
5. “Strategy analytics: internet of things now numbers 22 billion devices but where is the revenue?” strategy analytics online.
6. K. K. Patel, S. M. Patel, and P. Scholar, “Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges,” International journal of engineering science and computing, vol. 6, 2016.
7. O. Vermesan and P. Friess, Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems, River publishers, Denmark, 2013.
8. M. Rana, A. Shafiq, I. Altaf et al., “A secure and lightweight authentication scheme for next generation IoT infrastructure,” Computer Communications, vol. 165, pp. 85–96, 2021.Khader, R., & Eleyan, D. (2021). Survey of dos/ddos attacks in iot. Sustainable Engineering and Innovation, 3(1), 23-28.
9. J. Zhang and D. Tao, "Empowering Things With Intelligence: A Survey of the Progress, Challenges, and Opportunities in Artificial Intelligence of Things," in IEEE Internet of Things Journal, vol. 8, no. 10, pp. 7789-7817, 15 May15, 2021, doi: 10.1109/JIOT.2020.3039359.
10. H. Qin, S. Zawad, Y. Zhou, S. Padhi, L. Yang and F. Yan, "Reinforcement-Learning-Empowered MLaaS Scheduling for Serving Intelligent Internet of Things," in IEEE Internet of Things Journal, vol. 7, no. 7, pp. 6325-6337, July 2020, doi: 10.1109/JIOT.2020.2965103.
11. Y. Otoum, V. Chamola and A. Nayak, "Federated and Transfer Learning-Empowered Intrusion Detection for IoT Applications," in IEEE Internet of Things Magazine, vol. 5, no. 3, pp. 50-54, September 2022, doi: 10.1109/IOTM.001.2200048
12. A. Ata, M. A. Khan, S. Abbas, M. S. Khan and G. Ahmad, "Adaptive IoT Empowered Smart Road Traffic Congestion Control System Using Supervised Machine Learning Algorithm," in The Computer Journal, vol. 64, no. 11, pp. 1672-1679, Nov. 2019, doi: 10.1093/comjnl/bxz129.
13. M. B. Krishna, "Group-based incentive and penalizing schemes for proactive participatory data sensing in IoT networks," 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 2018, pp. 796-801, doi: 10.1109/WF-IoT.2018.835520.
14. A. Degada, H. Thapliyal and S. P. Mohanty, "Smart Village: An IoT Based Digital Transformation," 2021 IEEE 7th World Forum on Internet of Things (WF-IoT), New Orleans, LA, USA, 2021, pp. 459-463, doi: 10.1109/WF-IoT51360.2021.9594980. C. Sharma and N. K. Gondhi, "Communication Protocol Stack for Constrained IoT Systems," 2018 3rd International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Bhimtal, India, 2018, pp. 1-6, doi: 10.1109/IoT-SIU.2018.8519904.
15. S. Altayaran and W. Elmedany, "Security threats of application programming interface (API's) in internet of things (IoT) communications," 4th Smart Cities Symposium (SCS 2021), Online Conference, Bahrain, 2021, pp. 552-557, doi: 10.1049/icp.2022.0399.
16. N. A. Gunathilake, W. J. Buchanan and R. Asif, "Next Generation Lightweight Cryptography for Smart IoT Devices: : Implementation, Challenges and Applications," 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 2019, pp. 707-710, doi: 10.1109/WF-IoT.2019.8767250.
17. N. Shahid and S. Aneja, "Internet of Things: Vision, application areas and research challenges," 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2017, pp. 583-587, doi: 10.1109/I-SMAC.2017.8058246.
18. S. I. Soto-Ortiz, P. J. Salazar-Pérez and K. L. Guadalupe-Gallardo, "Development of a DAPP (decentralized application) on Rinkeby Network for the registration of Sensors of an Internet of Things (IoT) Environment," 2022 IEEE.

19. X. Wang, W. Luo, X. Bai and Y. Wang, "Research on Big Data Security and Privacy Risk Governance," 2021 International Conference on Big Data, Artificial Intelligence and Risk Management (ICBAR), Shanghai, China, 2021, pp. 15-18, doi: 10.1109/ICBAR55169.2021.00011.
20. Nishant Chaurasia, Prashant Kumar, A comprehensive study on issues and challenges related to privacy and security in IoT, e-Prime - Advances in Electrical Engineering, Electronics and Energy, Volume 4,2023,100158, ISSN 2772-6711. Mourade Azrour, Jamal Mabrouki, Azidine Guezzaz, Ambrina Kanwal, "Internet of Things Security: Challenges and Key Issues", Security and Communication Networks, vol. 2021, Article ID 5533843.
21. O. Vermesan and P. Friess, Internet of THINGS: Converging Technologies for Smart Environments and Integrated Ecosystems, River publishers, Denmark, 2013
22. M. Rana, A. Shafiq, I. Altaf et al., "A secure and lightweight authentication scheme for next generation IoT infrastructure," Computer Communications, vol. 165, pp. 85–96, 2021.
23. S. A. Chaudhry, K. Yahya, F. Al-Turjman, and M.-H. Yang, "A secure and reliable device access control scheme for IoT based sensor cloud systems," IEEE Access, vol. 8, pp. 139244–139254, 2020.
24. A. Irshad, S. A. Chaudhry, O. A. Alomari, K. Yahya, and N. Kumar, "A novel pairing-free lightweight authentication protocol for mobile cloud computing framework," IEEE Syst. J.vol. 99, pp. 1–9, 2020.
25. S. A. Chaudhry, M. S. Farash, N. Kumar, and M. H. Alsharif, "PFLUA-DIoT: a pairing free lightweight and unlinkable user access control scheme for distributed IoT environments," IEEE Syst. J.vol. 99, pp. 1–8, 2020.
26. M. B. Mu'azu, "SIMP-REAUTH: a simple multilevel real user remote authentication scheme for mobile cloud computing," in Proceedings of the Information and Communication Technology and Applications: Third International Conference, ICTA 2020, November 2020.
27. Zaidi, A., Karim, A. A., Mohiuddin, S., Khan, A., Syed, A., Jehangir, M., & Afzal, I. (2018). Dental Sensitivity Associated With Consumption Of Fizzy Drinks: A Cross Sectional Study. Pakistan Journal of Medicine and Dentistry, 7(4), 5-5.
28. S. -H. Park, D. Kim and S. -W. Lee, "A Tool for Security Risk Assessment for APT Attacks: using Scenarios, Security Requirements, and Evidence," 2023 IEEE 31st International Requirements Engineering Conference (RE), Hannover, Germany, 2023, pp. 363-364, doi: 10.1109/RE57278.2023.00053.
29. P. Napolitano, G. Rossi, M. Lombardi, F. Garzia, M. Ilariucci and G. Forino, "Threats Analysis and Security Analysis for Critical Infrastructures: Risk Analysis Vs. Game Theory," 2018 International Carnahan Conference on Security Technology (ICCST), Montreal, QC, Canada, 2018, pp. 1-5, doi: 10.1109/CCST.2018.8585725.
30. A. Yokotani, H. Mineno, K. Kosaka, M. Mitsuuchi, K. Ishibashi and T. Yokotani, "Low-Latency Processing of IoT Information in the IoT Platform Named "C-NAT"," in IEICE Communications Express, vol. 12, no. 12, pp. 620-623, December 2023, doi: 10.23919/comex.2023COL0017.
31. I. Froiz-Míguez, P. Fraga-Lamas and T. M. Fernández-CaraméS, "Design, Implementation, and Practical Evaluation of a Voice Recognition Based IoT Home Automation System for Low-Resource Languages and Resource-Constrained Edge IoT Devices: A System for Galician and Mobile Opportunistic Scenarios," in IEEE Access, vol. 11, pp. 63623-63649, 2023, doi: 10.1109/ACCESS.2023.3286391.
32. T. -T. -H. Le, R. W. Wardhani, D. S. C. Putranto, U. Jo and H. Kim, "Toward Enhanced Attack Detection and Explanation in Intrusion Detection System-Based IoT Environment Data," in IEEE Access, vol. 11, pp. 131661-131676, 2023, doi: 10.1109/ACCESS.2023.3336678
33. A. Saputhanthri, C. De Alwis and M. Liyanage, "Survey on Blockchain-Based IoT Payment and Marketplaces," in IEEE Access, vol. 10, pp. 103411-103437, 2022, doi: 10.1109/ACCESS.2022.3208688.
34. B. Soret et al., "Learning, Computing, and Trustworthiness in Intelligent IoT Environments: Performance-Energy Tradeoffs," in IEEE Transactions on Green Communications and Networking, vol. 6, no. 1, pp. 629-644, March 2022, doi: 10.1109/TGCN.2021.31387
35. N. M. Karie, N. M. Sahri, W. Yang, C. Valli and V. R. Kebande, "A Review of Security Standards and Frameworks for IoT-Based Smart Environments," in IEEE Access, vol. 9, pp. 121975-121995, 2021, doi: 10.1109/ACCESS.2021.3109886.
36. T. Kieras, J. Farooq and Q. Zhu, "I-SCRAM: A Framework for IoT Supply Chain Risk Analysis and Mitigation Decisions," in IEEE Access, vol. 9, pp. 29827-29840, 2021, doi: 10.1109/ACCESS.2021.3058338
37. M. Anedda et al., "Privacy and Security Best Practices for IoT Solutions," in IEEE Access, vol. 11, pp. 129156-129172, 2023, doi: 10.1109/ACCESS.2023.3331820.
38. T. Sauter and A. Treytl, "IoT-Enabled Sensors in Automation Systems and Their Security Challenges," in IEEE Sensors Letters, vol. 7, no. 12, pp. 1-4, Dec. 2023, Art no. 7500904, doi: 10.1109/LSENS.2023.3332404.

39. R. Pal et al., "Aggregate Cyber-Risk Management in the IoT Age: Cautionary Statistics for (Re)Insurers and Likes," in IEEE Internet of Things Journal, vol. 8, no. 9, pp. 7360-7371, 1 May1, 2021, doi: 10.1109/JIOT.2020.3039254.
40. M. A. Khatun, S. F. Memon, C. Eising and L. L. Dhirani, "Machine Learning for Healthcare-IoT Security: A Review and Risk Mitigation," in IEEE Access, vol. 11, pp. 145869-145896, 2023, doi: 10.1109/ACCESS.2023.3346320.
41. I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu and W. Ni, "Anatomy of Threats to the Internet of Things," in IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1636-1675, Secondquarter 2019, doi: 10.1109/COMST.2018.2874978.
42. Hussain, S.K., Ramay, S.A., Shaheer, H., Abbas T., Mushtaq M.A., Paracha, S., & Saeed, N. (2024). Automated Classification of Ophthalmic Disorders Using Color Fundus Images, Volume: 12, No: 4, pp. 1344-1348 DOI:10.53555/ks.v12i4.3153.
43. Tandon, R., Sayed, A., & Hashmi, M. A. (2023). Face mask detection model based on deep CNN technique using AWS. International Journal of Engineering Research and Applications www.ijera.com, 13(5), 12-19.
44. Zaidi, A., Karim, A. A., Mohiuddin, S., Khan, A., Syed, A., Jehangir, M., & Afzal, I. (2018). Dental Sensitivity Associated With Consumption Of Fizzy Drinks: A Cross Sectional Study. Pakistan Journal of Medicine and Dentistry, 7(4), 5-5.
45. Shah AM, Aljubayri M, Khan MF, Alqahtani J, Hassan MU, Sulaiman A, et al. ILSM: incorporated lightweight security model for improving QOS in WSN. Comput Syst Sci Eng. 2023;46(2):2471-2488 https://doi.org/10.32604/csse.2023.034951.
46. Abbas, M., Arslan, M., Bhatty, R. A., Yousaf, F., Khan, A. A., & Rafay, A. (2024). Enhanced Skin Disease Diagnosis through Convolutional Neural Networks and Data Augmentation Techniques. Journal of Computing & Biomedical Informatics, 7(01).