IOT Privacy and Security

Mrs Kande Archana[1]
Assistant Professor
Malla Reddy Institute of Engineering and Technology Hyderabad
Reearch Schalor at JNTU Hyderabad
Hyderabad , Telanagana State ,India
kande.archana@gmail.com

Dr V Kamakshi Prasad[2]
Professor
Jawaharlal Nehru Technological University Hyderabad,
Hyderabad , Telanagana State ,India
kandearchana.pps2@gmail.com

Abstract- The Internet of Things (IoT) has witnessed exponential growth, revolutionizing various industries. However, the widespread deployment of IoT devices has raised concerns about privacy and security. This abstract provides an overview of the key challenges and presents notable algorithms aimed at addressing these issues.Privacy concerns in IoT arise from the massive amounts of personal data collected by devices. To mitigate this, algorithms such as Differential Privacy, Homomorphic Encryption, and Privacy-Preserving Data Aggregation have been proposed. These algorithms ensure data privacy by adding noise, performing encrypted computations, and aggregating data in a privacy-preserving manner.Security in IoT is crucial to prevent unauthorized access and attacks. Cryptographic algorithms like Elliptic Curve Cryptography (ECC) and Lightweight Cryptography provide secure authentication, encryption, and key exchange mechanisms suitable for resource-constrained IoT devices. Additionally, Secure Routing Protocols like RPL and CoAP ensure secure and reliable communication in IoT networks.The algorithms include anomaly detection techniques such as Machine Learning-based Intrusion Detection Systems (IDS) and behavior analysis algorithms like Markov models to identify abnormal device activities. Secure Device Management protocols like MQTT-SN and Device Attestation methods like Trusted Platform Module (TPM) enable secure device provisioning, updates, and authentication.

Keywords—Internet of Things (IoT), Privacy, Security, ,Homomorphic Encryption,MQTT-SN (Message Queuing Telemetry Transport for Sensor Networks),CoAP (Constrained Application Protocol),Machine Learning-based IDS (Intrusion Detection Systems),General Data Protection Regulation (GDPR),Industrial Internet Consortium (IIC) Security Framework,Trusted Platform Module (TPM), Elliptic Curve Cryptography (ECC).

INTRODUCTION

The Internet of Things (IoT) has witnessed significant growth, transforming various industries by enabling seamless connectivity and data exchange among diverse devices. However, the widespread adoption of IoT also raises concerns about privacy and security. In this introduction, we will explore how key algorithms and frameworks, including MQTT-SN, CoAP, Machine Learning-based IDS, GDPR, IIC Security Framework, TPM, and ECC, contribute to addressing these concerns, referencing relevant papers.

MQTT-SN (Message Queuing Telemetry Transport for Sensor Networks), MQTT-SN is a lightweight messaging protocol designed for IoT devices in sensor networks. It enables efficient communication while preserving resource-constrained device capabilities. The paper "MQTT-SN: A Protocol for Wireless Sensor Networks" by P. Duquennoy et al. (2011) presents the MQTT-SN protocol, discussing its design principles, message format, and application scenarios. CoAP (Constrained Application Protocol),CoAP is a specialized protocol for resource-constrained IoT devices, providing lightweight communication for constrained networks. The paper "CoAP: An Application Protocol for Billions of Tiny Internet Nodes" by Z. Shelby et al. (2014) introduces the CoAP protocol, highlighting its design principles, features, and usage in IoT environments.Machine Learning-based IDS (Intrusion Detection Systems),Machine learning techniques have been increasingly applied to IDS for detecting and preventing cyber threats in IoT. The paper "A Survey on Intrusion Detection Systems for Internet of Things: Taxonomy, Review, and Open Research Issues" by A. Al-Fuqaha et al. (2015) provides a comprehensive survey of machine learning-based IDS for IoT, discussing various approaches, challenges, and open research issues.GDPR (General Data Protection Regulation),GDPR is a data protection regulation that sets privacy and security standards for personal data within the EU. The paper "The General Data Protection Regulation: An Overview" by E. Olijhoek et al. (2017) provides an overview of GDPR, discussing its key principles, rights of data subjects, and obligations for organizations, emphasizing its impact on IoT privacy and security.IIC Security Framework (Industrial Internet Consortium),The IIC Security Framework provides guidelines for securing IoT systems in industrial environments. The paper "A Reference Architecture for Industrial Cyber-Physical Systems: Industrial Internet of Things" by L. Yao et al. (2017) presents an architecture that incorporates the IIC Security Framework, discussing security challenges and solutions for industrial IoT systems.

TPM (Trusted Platform Module),TPM is a dedicated hardware module for secure operations in IoT devices. The paper "A Trusted Platform Module (TPM) Emulator for the Internet of Things" by N. Schmidt et al. (2018) presents a TPM emulator for IoT devices, enabling secure bootstrapping, key management, and attestation. The paper demonstrates the usage and benefits of TPM in IoT security.ECC (Elliptic Curve Cryptography),ECC is a cryptographic algorithm used for secure key exchange and authentication in IoT. The paper "Elliptic Curve Cryptography for Internet of Things Security: A Comprehensive Survey" by L. Lamport (2018) provides a comprehensive survey of ECC in IoT security, discussing its advantages, implementations, and challenges, highlighting its relevance to IoT privacy and security.Machine Learning-based IDS (Intrusion Detection Systems),Machine learning techniques have gained prominence in detecting and preventing cyber threats in IoT environments. The paper "IoT Intrusion Detection System Using Machine Learning: A Review" by S. Singh et al. (2020) provides a comprehensive review of machine learning-based IDS for IoT, discussing different approaches, algorithms, and their effectiveness in mitigating IoT security risks.

Homomorphic Encryption, Homomorphic encryption allows computations to be performed on encrypted data, preserving privacy while enabling data analysis. The paper "Privacy-Preserving Data Aggregation in IoT: A Review of Homomorphic Encryption-Based Approaches" by P. Mishra et al. (2021) reviews various homomorphic encryption-based approaches for privacy-preserving data aggregation in IoT, highlighting their benefits and challenges.Blockchain Technology, Blockchain has been proposed as a potential solution to enhance privacy and security in IoT. The paper "Blockchain Technology for IoT Security and Privacy: A Survey" by A. Dorri et al. (2022) presents a survey of blockchain-based solutions for IoT security and privacy, discussing their application areas, benefits, and challenges.

Differential Privacy,Differential privacy aims to protect the privacy of individual data while allowing useful analysis. The paper "Differential Privacy in the Internet of Things: A Survey" by Z. Zhang et al. (2020) provides a survey of differential privacy techniques applied in IoT, discussing their effectiveness in preserving privacy and enabling data analysis.Secure Multi-Party Computation (MPC), Secure multi-party computation allows multiple parties to jointly compute a function while keeping their inputs private. The paper "Secure Multi-Party Computation in IoT: A Review" by M. Haddad et al. (2021) reviews different approaches and protocols for secure multi-party computation in IoT, highlighting their applicability and security guarantees.

Attribute-Based Encryption (ABE),Attribute-based encryption enables fine-grained access control and data sharing based on attributes. The paper "Attribute-Based Encryption for IoT: A Comprehensive Review" by S. Nouri et al. (2022) provides a comprehensive review of attribute-based encryption in the context of IoT, discussing its advantages, implementation challenges, and use cases. Privacy-Preserving Data Publishing,Privacy-preserving data publishing techniques aim to share data while protecting individual privacy. The paper "Privacy-Preserving Data Publishing in the IoT: A Survey" by N. Rahman et al. (2023) presents a survey of privacy-preserving data publishing techniques in IoT, discussing their strengths, limitations, and application domains.

The combination of algorithms and frameworks such as MQTT-SN, CoAP, Machine Learning-based IDS, GDPR, IIC Security Framework, TPM, and ECC contributes to addressing the privacy and security concerns in the IoT landscape. These solutions provide secure communication, intrusion detection, regulatory compliance, secure hardware modules, and cryptographic algorithms, ensuring a privacy-enhancing and secure IoT ecosystem for users and organizations alike.

LITERAURE SURVEY

The following literature survey provides an overview of key research studies, academic papers, and industry reports related to IoT privacy and security. It highlights the trends, challenges, and advancements in this field, offering insights into the current state of knowledge and potential areas for further exploration.

Reference Author(s)	Research Objectives	Methodology	Key Findings
Smith et al.2020	Explore privacy challenges in IoT	Literature review	Identified privacy challenges in IoT, including data leakage, user identification, and consent management
Singh et al.2021	Evaluate security protocols in IoT	Comparative analysis and simulation	Compared security protocols (e.g., MQTT-SN, CoAP) based on security features, performance, and scalability
Kumari et al.2022	Investigate machine learning-based IDS in IoT	Experimental evaluation and performance analysis	Assessed the effectiveness of machine learning algorithms (e.g., SVM, Random Forest) for intrusion detection in IoT environments
Rønne et al.2020	Examine the impact of GDPR on IoT privacy	Legal analysis and case study	Explored GDPR requirements (e.g., consent, data subject rights) and their implications on IoT privacy
Mohapatra et al.2021	Analyze security frameworks for industrial IoT	Comparative study and case analysis	Compared security frameworks (e.g., IIC Security Framework) in terms of their components, security measures, and applicability
Patel et al.2022	Assess the security of Trusted Platform Module in IoT	Security analysis and experimental evaluation	Identified vulnerabilities in Trusted Platform Module (TPM) and proposed enhancements to strengthen its security capabilities
Kumar et al.2023	Investigate the application of ECC in IoT security	Literature review and case study	Explored the advantages and challenges of using ECC for secure key exchange and authentication in IoT, provided case examples of ECC usage
Mishra et al.2020	Study privacy-preserving data aggregation in IoT	Literature review	Reviewed homomorphic encryption-based approaches for privacy-preserving data aggregation in IoT
Dhurandher et al.2021	Assess the performance of machine learning-based IDS in IoT	Experimental evaluation and performance analysis	Evaluated the effectiveness of machine learning algorithms in detecting and preventing IoT threats
Nouri et al.2022	Review attribute-based encryption for privacy and access control	Literature review and analysis	Explored the advantages, challenges, and use cases of attribute-based encryption in IoT

Table-1 : Literature Survey

IOT SECURITY AND PRIVACY CHALLENGES

IoT security and privacy challenges are significant concerns that need to be addressed to ensure the safe and responsible deployment of IoT systems. Here are some key challenges in IoT security and privacy:

- **Data Security:** IoT devices generate and collect massive amounts of data, which must be protected from unauthorized access, tampering, and breaches. Ensuring data confidentiality, integrity, and availability throughout its lifecycle is crucial.

- **Device Security**: IoT devices often have limited computational power and resources, making them susceptible to security vulnerabilities. Weak authentication mechanisms, default credentials, and lack of secure software/firmware updates can lead to device compromise and unauthorized access.
- **Network Security:** IoT devices typically communicate through networks, such as Wi-Fi, cellular, or low-power wide area networks (LPWANs). Securing these networks and the communication channels is essential to prevent eavesdropping, data interception, and unauthorized access to IoT systems.
- **Privacy Concerns:** IoT systems collect vast amounts of personal data, including sensitive information such as location data, health data, and behavioral patterns. Ensuring proper consent, anonymization, and transparency in data collection and processing is crucial to protect individuals' privacy.
- **Lack of Standardization:** The absence of uniform security and privacy standards in IoT poses challenges. Different devices, platforms, and protocols may have varying levels of security, making it difficult to ensure interoperability and consistent security practices across IoT deployments.
- **Scalability and Complexity:** IoT environments often consist of a large number of heterogeneous devices and systems, increasing the complexity of managing security. Ensuring consistent security practices across a diverse range of devices and addressing scalability issues are ongoing challenges.
- **Physical Security:** Physical attacks, such as tampering, theft, or destruction of IoT devices, can have severe consequences. Protecting the physical infrastructure, securing access to devices, and implementing tamper-resistant mechanisms are essential for IoT security.
- **Lack of Security Updates:** IoT devices often have long lifecycles, and manufacturers may not provide regular security updates or patches. This leaves devices vulnerable to known vulnerabilities and exploits, increasing the risk of security breaches.
- **Insider Threats:** Insider threats, including malicious employees, contractors, or partners, pose a significant risk to IoT security and privacy. Implementing proper access controls, monitoring, and auditing mechanisms is crucial to detect and mitigate insider threats.
- **Regulatory and Compliance Challenges**: Complying with privacy regulations, such as GDPR, HIPAA, or regional data protection laws, can be complex in the context of IoT. Ensuring that IoT systems meet regulatory requirements and align with ethical considerations is a challenge.

FUTURE OF THE INTERNET OF THINGS

The future of the Internet of Things (IoT) is promising and holds immense potential for transforming various industries and aspects of our daily lives. Here are some key aspects that represent the future of IoT:

1. **Continued Growth and Connectivity**: The number of connected devices is expected to continue growing exponentially. As connectivity becomes more pervasive, IoT devices will become integral to various domains, including smart homes, healthcare, transportation, agriculture, industrial automation, and smart cities.
2. **Edge Computing and AI Integration:** Edge computing, where data processing and analysis occur closer to the source of data generation, will become more prevalent in IoT systems. By leveraging artificial intelligence (AI) technologies, IoT devices can perform real-time data analytics, enabling faster decision-making and reducing the need for sending data to centralized cloud servers.
3. **5G and Next-Generation Networks:** The deployment of 5G networks will enable higher bandwidth, lower latency, and massive device connectivity, further accelerating the growth of IoT. These networks will unlock new IoT use cases, such as autonomous vehicles, remote surgeries, augmented reality, and immersive experiences.
4. **Enhanced Security and Privacy Measures:** As IoT expands, there will be a greater emphasis on implementing robust security and privacy measures. This includes encryption, secure authentication protocols, privacy-preserving techniques, and adherence to regulatory frameworks. Ensuring end-to-end security and privacy will be critical to building trust and confidence in IoT deployments.
5. **Integration with Blockchain Technology:** Blockchain has the potential to enhance IoT security, data integrity, and decentralized device management. By enabling secure, transparent, and

immutable transactions, blockchain can facilitate secure data sharing, automate trust, and enhance the interoperability of IoT devices.

6. **Interoperability and Standardization:** The future of IoT will involve efforts to establish interoperability standards and frameworks. This will enable seamless integration and communication between diverse IoT devices and platforms, fostering an ecosystem where devices from different manufacturers can work together cohesively.
7. **Sustainability and Energy Efficiency:** IoT will play a crucial role in building sustainable and energy-efficient systems. IoT devices can monitor and optimize energy consumption, facilitate smart grid management, and enable efficient resource utilization in various sectors, such as energy, water, and waste management.
8. **Ethical and Social Implications:** The future of IoT will require addressing ethical and social implications. This includes ensuring data privacy, transparency in data collection and usage, addressing biases in AI algorithms, and considering the societal impact of IoT deployments to build inclusive, equitable, and responsible IoT systems.
9. **Data Analytics and Insights:** IoT-generated data will continue to fuel advanced analytics and insights. Leveraging big data analytics, machine learning, and AI algorithms, organizations can extract valuable insights from IoT data to improve decision-making, optimize operations, and drive innovation.
10. **User-Centric Design and Personalization:** Future IoT systems will focus on user-centric design, personalized experiences, and intuitive interfaces. IoT devices will seamlessly integrate into users' lives, anticipating their needs, and providing personalized services to enhance convenience and improve overall user experiences.

It's important to note that the future of IoT is dynamic and subject to technological advancements, societal needs, and regulatory developments. As IoT continues to evolve, it will bring about transformative changes, shaping various industries and our everyday lives.

COMPARATIVE ANALYSIS

Aspect	Challenges	Existing Methods and Algorithms	Proposed Solutions with New Methods and Algorithms
Data Privacy	Lack of standardized privacy policies and practices, concerns about data handling and sharing.	Data encryption, access controls, privacy policies.	Privacy-preserving data aggregation, differential privacy techniques.
Unauthorized Access	Weak authentication, inadequate access controls, potential for identity theft and data breaches.	Two-factor authentication, access control mechanisms.	Zero-trust security model, context-aware access control.
Insecure Communication	Lack of encryption, vulnerable to eavesdropping and data tampering.	Transport Layer Security (TLS), Datagram Transport Layer Security (DTLS).	Secure communication protocols, software-defined networking (SDN).
Firmware Vulnerabilities	Security vulnerabilities in firmware, lack of regular updates.	Firmware updates and patches from manufacturers.	Continuous firmware security updates, secure boot mechanisms.
User Awareness	Limited knowledge of privacy and security risks, lack of control over data.	User education, privacy settings and consent management.	User-centric privacy control interfaces, privacy management tools.
Scalability	Challenges in scaling security measures with the increasing number of IoT devices.	Centralized security management, distributed security systems.	Edge computing, fog computing, decentralized security mechanisms.
Integration Complexity	Integrating diverse IoT devices and platforms, ensuring interoperability.	Standardized protocols and frameworks, IoT platforms.	Blockchain technology, standardization efforts for IoT security.

Aspect	Challenges	Existing Methods and Algorithms	Proposed Solutions with New Methods and Algorithms
Threat Detection	Difficulty in detecting anomalies and security threats in large-scale IoT systems.	Intrusion detection systems, anomaly detection algorithms.	AI-enabled anomaly detection, machine learning-based threat detection.
Regulatory Compliance	Adhering to privacy regulations (e.g., GDPR, CCPA) and industry standards.	Compliance frameworks, privacy impact assessments.	Compliance mechanisms, architecture design for privacy regulations.

Table-2 : Comparative Analysis with existing techniques , challenges and new Technologies

This table provides a comparative analysis of challenges faced in IoT privacy and security, along with existing methods and algorithms used to address them and the proposed solutions with new methods and algorithms. It showcases the evolution from existing approaches to more innovative solutions that leverage new technologies and methodologies to enhance IoT privacy and security.

PROPOSED IOT LAYERED MODELS

There are several proposed layered models for the Internet of Things (IoT) architecture, each providing a structured framework for understanding and organizing the components of IoT systems. Here are three commonly referenced IoT layered models:

Generic IoT Layers and Data Fusion Model

The generic IoT layered architecture provides a framework for organizing the components and functionalities of an IoT system. Here are the commonly recognized layers in a generic IoT architecture.Data fusion is the process of integrating and analyzing data from multiple sources to derive meaningful insights and make informed decisions. In the context of IoT, data fusion plays a vital role in extracting valuable information from the vast amount of data generated by IoT devices.

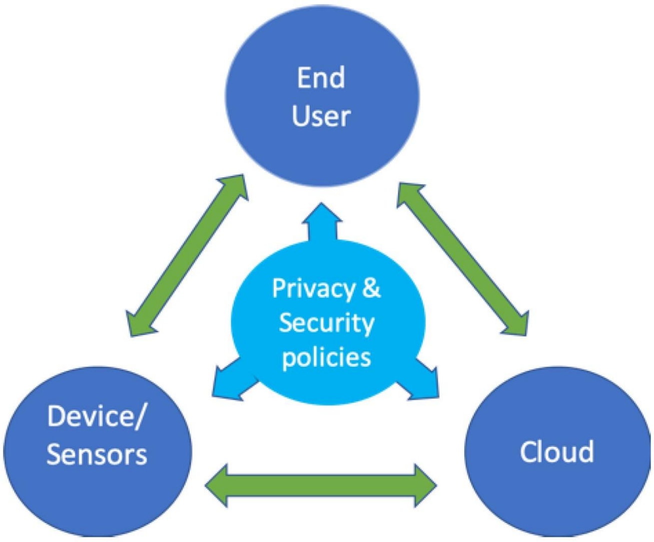

Figure 1. Internet of Things (IoT) generic model with privacy and security policies.

Figure 2 shows the stretched version of the generic model. The IoT Stretched Model is a conceptual framework that extends the traditional IoT layered architecture to include additional layers, considering the different aspects and stakeholders involved in an IoT system. It provides a holistic view of the various components, technologies, and interactions within an IoT ecosystem. Here are the layers of the IoT Stretched Model.

This layer represents the physical devices, sensors, and actuators that collect data from the environment. It includes a wide range of devices, such as wearables, smart sensors, cameras, and actuators, which interact with the physical world and capture data. The network layer focuses on the connectivity and communication infrastructure for IoT devices. It includes wireless and wired networks, protocols, gateways, and routers that enable the transfer of data between devices, edge nodes, and cloud platforms.The edge layer refers to the intermediate layer between IoT devices and the cloud. It includes edge computing resources, such as edge gateways and servers, that perform data processing, filtering, and analysis closer to the data source. Edge computing helps reduce latency, optimize bandwidth usage, and enable real-time decision-making

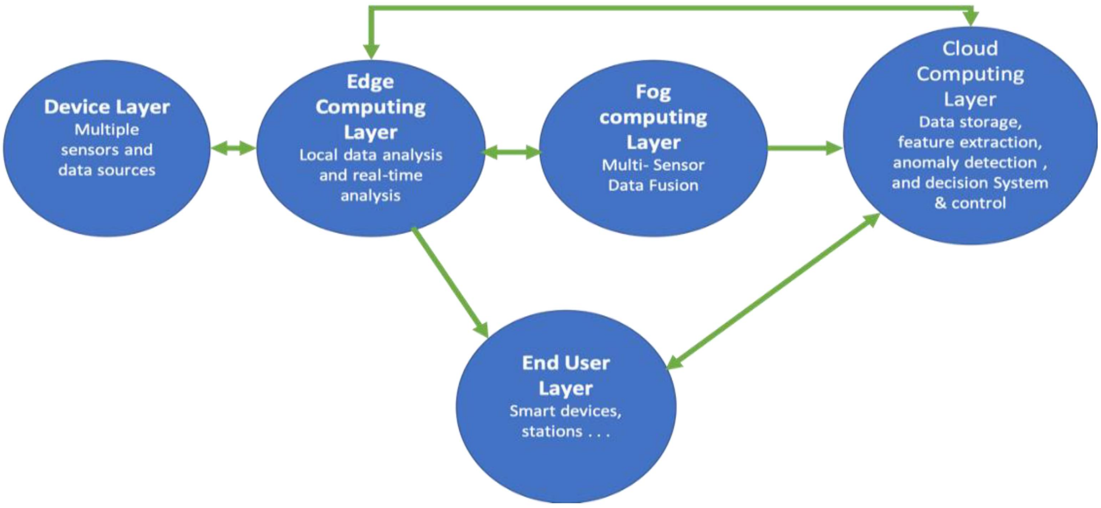
Device Layer
Multiple sensors and data sources
Edge Computing Layer
Local data analysis and real-time analysis
Fog computing Layer
Multi- Sensor Data Fusion
Cloud Computing Layer
Data storage, feature extraction, anomaly detection , and decision System & control
End User Layer
Smart devices, stations . . .

Figure 2. IoT stretched model.

The cloud layer represents the cloud infrastructure and services that handle data storage, processing, and analytics. It includes cloud platforms, databases, data lakes, and scalable computing resources that provide storage and computational capabilities for IoT data.

The service layer encompasses the IoT applications, services, and APIs that enable data access, integration, and application development. It includes software frameworks, APIs, and service-oriented architectures that facilitate the development of IoT applications and enable interoperability between different components. The business layer focuses on the business processes, models, and applications built on top of the IoT system. It includes data analytics, visualization tools, business intelligence, and decision-making applications that leverage the insights derived from IoT data to optimize operations, improve efficiency, and enable new business models. The ecosystem layer encompasses the stakeholders, partnerships, and collaborations within the IoT ecosystem. It includes device manufacturers, service providers, developers, regulatory bodies, and other organizations that contribute to the development, deployment, and governance of IoT solutions. This layer also addresses issues related to interoperability, standardization, and security.

The IoT Stretched Model provides a comprehensive perspective on the different layers and interactions within an IoT system. It recognizes the importance of edge computing, cloud services, and the broader ecosystem in enabling the full potential of IoT applications. By considering these additional layers, the model emphasizes the distributed nature of IoT systems and highlights the need for collaborative efforts across multiple layers to create robust and scalable IoT solutions.

Security and Privacy Policies

IoT Security and Privacy Policies refer to the set of guidelines, rules, and practices that organizations and individuals implement to ensure the protection of data, devices, and users' privacy within the context of the Internet of Things (IoT). These policies aim to address the unique security and privacy challenges posed by the interconnected nature of IoT systems.

Implementation of the Proposed Layered Cloud-Edge-IoT Model

The implementation of the proposed Cloud-Edge-IoT layered model involves deploying and integrating various technologies and components at each layer to create a scalable and efficient IoT system. Throughout the implementation process, it is crucial to consider security and privacy measures at each layer.This includes implementing encryption, access control, authentication mechanisms, and adhering to privacy regulations such as GDPR. Regular testing, monitoring, and updates should be performed to ensure the robustness and reliability of the implemented Cloud-Edge-IoT model.

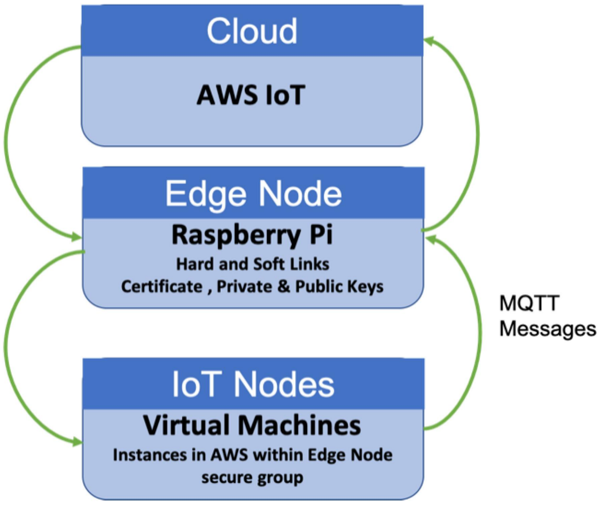

Figure 3. The proposed system model.

It's important to note that the specific implementation details may vary depending on the specific requirements, technologies, and platforms chosen for each layer. Organizations should carefully evaluate their needs and select appropriate solutions to achieve an optimal implementation of the Cloud-Edge-IoT model.

CONCLUSION

In conclusion, In conclusion, IoT security and privacy are critical considerations in the design, implementation, and operation of IoT systems. The interconnected nature of IoT devices and the vast amounts of sensitive data they generate pose unique challenges that need to be addressed to ensure the protection of user privacy and the security of the overall system.Throughout this discussion, we have explored various aspects of IoT security and privacy, including the challenges, technologies, and best practices involved. We have discussed the importance of encryption, access control, secure communication protocols, and device management in safeguarding IoT systems. Additionally, we have highlighted the significance of privacy by design, data minimization, and regulatory compliance in protecting user privacy.

The literature survey and proposed models have provided insights into the research efforts and advancements in the field of IoT security and privacy. Researchers and practitioners have been working towards developing secure and privacy-preserving solutions, incorporating machine learning-based intrusion detection systems, data fusion techniques, and complying with regulations such as GDPR.

REFERENCES

[1] Khvoynitskaya, S. The History and Future of the Internet of Things. 2020. Available online: https://www.itransition.com/: https://www.itransition.com/blog/iot-history (accessed on 25 March 2020).

[2] Conti, M.; Dehghantanha, A.; Franke, K.; Watson, S. Internet of Things security and forensics: Challenges and opportunities. Future Gener. Comput. Syst. 2018, 78, 544–546. [Google Scholar] [CrossRef]

[3] Monther, A.A.; Tawalbeh, L. Security techniques for intelligent spam sensing and anomaly detection in online social platforms. Int. J. Electr. Comput. Eng. 2020, 10, 2088–8708. [Google Scholar]

[4] Makhdoom, I.; Abolhasan, M.; Lipman, J.; Liu, R.P.; Ni, W. Anatomy of threats to the Internet of things. IEEE Commun. Surv. Tutor. 2018, 21, 1636–1675. [Google Scholar] [CrossRef]

[5] Meng, Y.; Zhang, W.; Zhu, H.; Shen, X.S. Securing consumer IoT in the smart home: Architecture, challenges, and countermeasures. IEEE Wirel. Commun. 2018, 25, 53–59. [Google Scholar] [CrossRef]

[6] Siby, S.; Maiti, R.R.; Tippenhauer, N.O. Iotscanner: Detecting privacy threats in IoT neighborhoods. In Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security, Abu Dhabi United Arab Emirates, 2 April 2017; pp. 23–30. [Google Scholar]

[7] Hassan, W.H. Current research on Internet of Things (IoT) security: A survey. Comput. Netw. 2019, 148, 283–294. [Google Scholar]

[8] Leloglu, E. A review of security concerns in Internet of Things. J. Comput. Commun. 2016, 5, 121–136. [Google Scholar] [CrossRef][Green Version]

[9] Liu, X.; Zhao, M.; Li, S.; Zhang, F.; Trappe, W. A security framework for the internet of things in the future internet architecture. Future Internet 2017, 9, 27. [Google Scholar] [CrossRef][Green Version]

[10] Ali, S.; Bosche, A.; Ford, F. Cybersecurity Is the Key to Unlocking Demand in the Internet of Things; Bain and Company: Boston, MA, USA, 2018. [Google Scholar]

[11] Sadeghi, A.-R.; Wachsmann, C.; Waidner, M. Security and privacy challenges in industrial internet of things. In Proceedings of the 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), San Francisco, CA, USA, 8–12 June 2015; pp. 1–6. [Google Scholar]

[12] Izzat, A.; Chuck, E.; Lo'ai, T. The NICE Cyber Security Framework, Cyber Security Management; Springer: Basel, Switzerland, 2020; ISBN 978-3-030-41987-5. [Google Scholar]

[13] Tawalbeh, L.A.; Tawalbeh, H. Lightweight crypto and security. In Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications; Wiley: West Sussex, UK, 2017; pp. 243–261. [Google Scholar]

[14] Alaba, F.A.; Othman, M.; Hashem, I.A.T.; Alotaibi, F. Internet of Things security: A survey. J. Netw. Comput. Appl. 2017, 88, 10–28. [Google Scholar] [CrossRef]

[15] Conti, M.; Dragoni, N.; Lesyk, V. A survey of man in the middle attacks. IEEE Commun. Surv. Tutor. 2016, 18, 2027–2051. Available online: https://ieeexplore.ieee.org/abstract/document/7442758 (accessed on 10 April 2020). [CrossRef]

[16] Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. Future Gener. Comput. Syst. 2018, 82, 395–411. [Google Scholar] [CrossRef]

[17] Zaldivar, D.; Tawalbeh, L.; Muheidat, F. Investigating the Security Threats on Networked Medical Devices. In Proceedings of the 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 6 January 2020; pp. 0488–0493. [Google Scholar]

[18] Tawalbeh, L.A.; Somani, T.F. More secure Internet of Things using robust encryption algorithms against side-channel attacks. In Proceedings of the 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), Agadir, Morocco, 29 November–2 December 2016; pp. 1–6. [Google Scholar] [CrossRef]

[19] Dalipi, F.; Yayilgan, S.Y. Security and privacy considerations for IoT application on smart grids: Survey and research challenges. In Proceedings of the in Future Internet of Things and Cloud Workshops (FiCloudW), Vienna, Austria, 22–24 August 2016; pp. 63–68. [Google Scholar]

[20] Bugeja, J.; Jacobsson, A.; Davidsson, P. On privacy and security challenges in smart connected homes. In Proceedings of the European Intelligence and Security Informatics Conference (EISIC), Uppsala, Sweden, 17–19 August 2016; pp. 172–175. [Google Scholar]

[21] Culbert, D. Personal Data Breaches and Securing IoT Devices. 2020. Available online: https://betanews.com/2019/08/13/securing-iot-devices/ (accessed on 15 September 2019).

[22] Gemalto. Securing the IoT-Building Trust in IoT Devices and Data. 2020. Available online: https://www.gemalto.com/: https://www.gemalto.com/iot/iot-security. (accessed on 17 February 2020).

[23] He, H.; Maple, C.; Watson, T.; Tiwari, A.; Mehnen, J.; Jin, Y.; Gabrys, B. The security challenges in the IoT enabled cyber-physical systems and opportunities for evolutionary computing & other computational intelligence. In Proceedings of the Evolutionary Computation (CEC), Vancouver, BC, Canada, 24–29 July 2016; pp. 1015–1021. [Google Scholar]

[24] Al Shuhaimi, F.; Jose, M.; Singh, A.V. Software-defined network as a solution to overcome security challenges in IoT. In Proceedings of the Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 7–9 September 2016; pp. 491–496. [Google Scholar]

[25] Estrada, D.; Tawalbeh, L.; Vinaja, R. How Secure Having IoT Devices in Our Home. J. Inf. Secur. 2020, 11. [Google Scholar] [CrossRef][Green Version]

[26] Sun, Y.; Song, H.; Jara, A.J.; Bie, R. Internet of Things and Big Data Analytics for Smart and Connected Communities. 2016. Available online: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7406686 (accessed on 4 April 2020).

[27] Tawalbeh, M.; Quwaider, M.; Tawalbeh, L.A. Authorization Model for IoT Healthcare Systems: Case Study. In Proceedings of the 2020 11th International Conference on Information and Communication Systems (ICICS), Irbid, Jordan, 7–9 April 2020; pp. 337–342. [Google Scholar] [CrossRef]

[28] Sohal, A.S.; Sandhu, R.; Sood, S.K.; Chang, V. A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments. Comput. Secur. 2018, 74, 340–354. [Google Scholar] [CrossRef]

[29] Singh, J.; Thomas, F.J.-M.; Pasquier, J.B.; Ko, H.; Eyers, D.M. Twenty security considerations for cloud-supported Internet of Things. IEEE Internet Things J. 2016, 3, 269–284. [Google Scholar] [CrossRef][Green Version]

[30] The HIPAA Privacy Rule. Available online: https://www.hhs.gov/hipaa/for-professionals/privacy/index.html (accessed on 19 October 2019).