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- TPrivacy and security are among the significant challenges of the Internet of Things (IoT). Improper device updates, lack of efficient and robust security protocols, user unawareness, and famous active device monitoring are among the challenges that IoT is facing. In this work, we are exploring the background of IoT systems and security measures, and identifying (a) different security and privacy issues, (b) approaches used to secure the components of IoT-based environments and systems, (c) existing security solutions, and (d) the best privacy models necessary and suitable for different layers of IoT driven applications. In this work, we proposed a new IoT layered model: generic and stretched with the privacy and security components and layers identification. The proposed cloud/edge supported IoT system is implemented and evaluated. The lower layer represented by the IoT nodes generated from the Amazon Web Service (AWS) as Virtual Machines. The middle layer (edge) implemented as a Raspberry Pi 4 hardware kit with support of the Greengrass Edge Environment in AWS. We used the cloud-enabled IoT environment in AWS to implement the top layer (the cloud). The security protocols and critical management sessions were between each of these layers to ensure the privacy of the users' information. We implemented security certificates to allow data transfer between the layers of the proposed cloud/edge enabled IoT model. Not only is the proposed system model eliminating possible security vulnerabilities, but it also can be used along with the best security techniques to countermeasure the cybersecurity threats facing each one of the layers; cloud, edge, and IoT.

Keywords—Internet of Things (IoT), Privacy, Security, Data encryption,Authentication,Firmware updates,Privacy by Design,Network Configuration,User consent,User control,Monitoring,Intrusion detection,Physical security,Vendor accountability,User awareness,Best practices,Regulations,Data confidentiality,Data integrity,Trust.

INTRODUCTION

The Internet of Things (IoT) refers to a concept of connected objects and devices of all types over the Internet wired or wireless. The popularity of IoT or the Internet of Things has increased rapidly, as these technologies are used for various purposes, including communication, transportation, education, and business development. IoT introduced the hyperconnectivity concept, which means organizations and individuals can communicate with each other from remote locations effortlessly. Kevin Ashton invented the term 'IoT' in the year 1999 for promoting the Radio Frequency Identification (RFID) concept, which includes embedded sensors and actuators. However, the original idea was introduced in the 1960s. During that period, the idea was called pervasive computing or embedded Internet. Ashton presented the IoT concept to improve supply chain activities. However, diverse functionalities of IoT has helped it to gain strong popularity in the summer of 2010. The Chinese government gave strategic priority on IoT by introducing a five-year plan. About 26.66 billion IoT devices exist in the current world [1]. The mass explosion started in 2011 with the introduction of home automation, wearable devices, and smart energy meters. The rapid explosion of IoT has benefitted organizations and in various ways improved market research and business strategies. Similarly, IoT has improved the lifestyle of individuals by introducing automated services. However, such an uncontrolled explosion has increased privacy and security challenges.

The unconscious use, not changing passwords, and the lack of device updates have increased cybersecurity risks and access to malicious applications to the IoT systems' sensitive data. Such inappropriate security practices increase the chances of a data breach and other threats. Most of the security professionals consider IoT as the vulnerable point for cyber attacks due to weak security protocols and policies. Even though several security mechanisms were developed to protect IoT devices from cyber attacks, security guidelines are not appropriately documented [2]. Thereby, end-users could not utilize protective measures to avert data attacks. Hackers developed different kinds of malware to infect the IoT devices since the eve of 2008. They designed various phishing techniques to provoke the employees or individuals to share sensitive data [3]. Therefore, corporate workstations and personal devices often face privacy violations due to high-profile attacks. If device manufacturers and security experts assess the cyber threats accurately, they can develop an efficient protective mechanism to prevent or neutralize cyber threats.

IoT enabled devices have been used in industrial applications and for multiple business purposes [4]. The apps help these businesses to attain a competitive edge over their competitors. However, due to the excessive adoption of various smart devices with data sharing and integration, the privacy and data breach becomes a significant concern to most businesses, as it interrupts the flow of work, activities, and network services. It is essential to have professionals to overcome these threat concerns and develop comprehensive security measures and policies to protect their business assets and ensure services continuity and stability. For example, smart kitchen home IoT enabled appliances connected to the local network can be a source of the breach for hackers to get access to the business and/or personally sensitive data or to manipulate and interrupt the business workflow.

Every day new technologies emerge, or changes are made to existing ones. Consider the latest advances in the 5G network, for example. 5G is expected to play an essential role in the IoT systems and applications. It is getting the researchers' attention and curiosity about the possible security and privacy risks, with its high frequency and bandwidth. Yet, the short wavelength imposes a change in the infrastructure, hence the need for more base stations to cover the same area covered by other wireless technology. This new structure imposes more threats, such as fake base stations. It is essential to understand the security risks and potential solutions.

In this work, we aim to provide an overview of the IoT applications, benefits, and potential risks. Additionally, to build a framework to study and further develop best security practices by either implementing and analyzing current existing schemes or developing new ones. Based on the findings, we provide recommendations to avoid such risks and to remedy the possible security vulnerabilities. This work will guide regulatory agencies to continue enforcing policies, educating end-users and entities, and stakeholders involved in IoT to develop and apply more appropriate security and privacy measures.

We built our model using Amazon Web Service (AWS) as proof of concept, which later translated to actual physical systems of sensors nodes mimicking general IoT structure. By making the system, we can deploy and study different security approaches by building real sceneries and benchmarks.
We adopted a narrative review methodology to explore the history and background of the IoT systems, their security and privacy issues, and the corresponding countermeasures. We proposed our own view of the generic and stretched IoT model and its privacy and security concerns. We built and studied a cloud/edge supported IoT model consisted of a virtual machine (sensors), and edge node (Raspberry Pi), and cloud services (AWS). This setup was designed to evaluate the model we proposed in the following sections in this paper. Our work does not provide details on the different IoT applications (smart health, smart cities, supply chain, transportations, etc.); their features, advantages, and challenges, or the possible security risks or threats among these applications. The literature is rich with such content. In this work, we preferred to have a general overview with proof of concept and lay the ground for further analysis and investigations.

The rest of this paper organized as follows: the next section presents a literature review followed by IoT security and privacy challenges. In Section 4, we discuss the future of the Internet of Things. Section 5 presents the proposed cloud/edge supported IoT layered models: generic and stretched with the privacy and security components and layers identification. This section also shows the implementation of the proposed model using AWS cloud and edge environments and Raspberry Pi 4 kit. Section 6 concludes this work.

LITERAURE SURVEY

The authors in [5] stated that there are various challenges, such as jamming and spoofing attacks and other unauthorized access, which have compromised the integrity of the user's data. There are potential solutions that can help the individual to implement various security measures that can help to secure their IoT devices. According to [6], various privacy threats have emerged in the present time, and they can penetrate IoT Technologies and their integrated network. It is not easy to manage the security of IoT devices in businesses and organizations. The organizations must deploy monitoring and scanning tools for all the IoT devices that could detect any kind of threats related to privacy and try to mitigate the risk of being breached. Traffic interceptors and analyzers help identify and investigate various cyber threats.

There are various studies as well as services that have been conducted on the current trends in IoT security [7]. Multiple services have presented some of the challenges or attack vectors to various IoT devices and their guards. Various simulation tools, modelers, and the availability of numerous platforms that can confirm this security protocol can also help in producing the protocol related to novel IoT security. It is fair to say that there has been rapid progress in terms of research related to IoT security and various simulation tools as well as modelers have supported this research. If the IoT devices failed, then the issues will be severe.

The authors in [8] believe that, despite the enormous benefits the users are getting from the Internet of Things, there are challenges that come along with it that need to be looked at. Cybersecurity and privacy risks are the primary concerns that have been cited. These two are posing a massive predicament for many business organizations as well as public organizations. Prevalent high-profile cybersecurity attacks have demonstrated the vulnerabilities of IoT technologies. This is simply because the interconnectivity of networks in the Internet of Things brings along accessibility from anonymous and untrusted Internet, requiring novel security solutions. On the other hand, it is important to emphasize the standards and basic principles of the IoT Cyber Security Framework when it comes to implementing the IoT security system. According to [9], one of the most important measures to consider is the termination of a contract consisting of different devices with different communication protocols. The difference in protocols hinder separate service contracts from implementation and are fundamental elements that must be present in the cybersecurity structure of every Internet of Things. He demonstrated that to ensure the reliability of the IoT framework in the cybersecurity arena, some small steps need to be taken to help mitigate the challenges of IoT cybersecurity. In addition, the authors in [9] showed that scalability is also an essential measure of the success of the cybersecurity Internet of Things framework. Analysts said the IoT environment needs to be scalable enough to handle a billion Internet-related and cybersecurity challenges. In addition, the magazine showed that the IoT cybersecurity environment should also support testability, such as integration testing, component testing, system testing, and compliance testing, effectively reducing challenges and risks.

In the same context, the authors in [10] described some of the current IoT cybersecurity solutions. Some basic security measures are implemented by the supplier, and state that it is not profitable for the supplier to produce high-quality solutions. In the case of cybersecurity of the Internet of Things, companies are unlikely to develop the right solution.

Moreover, the authors in [11] describe the currently embedded mobile and cyber-physical systems as ubiquitous, from industrial control systems, modern vehicles to critical infrastructure. Current trends and initiatives, such as Industry 4.0 and the Internet of Things (IoT), promise innovative business models and new user experiences through strong connectivity and the effective use of new generations of embedded devices. These systems generate, process, and exchange large amounts of relevant data. Security and confidential beliefs that make cyber attacks an attractive target for the Internet of Things system cause physical harm and disrupt people’s lives. Cybersecurity and privacy are important because they can pose a threat. The complexity of these systems and the potential impact of cyber attacks pose new threats to related industrial IoT systems. Possible solutions to security and privacy challenges are general security frameworks for industrial IoT systems. Current IoT systems have not improved enough to secure the desired functions.

Therefore, there has been extreme significance in the study and research of various security issues in IoT. One of the main objectives in terms of IoT security is to provide privacy, confidentiality, and to ensure that every user can get better protection, infrastructures, and a guarantee to the availability of various services offered by the ecosystem of IoT. Therefore, the research in various IoT security is gaining necessary momentum with the help of different simulation tools as well as multiple computational platforms [12].

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	Research Objective	Methodology	Key Findings
Alaba et al. (2017)	Security measures, including encryption, authentication, and access control mechanisms	comprehensive survey of IoT security and privacy issues.	Identified various threats and vulnerabilities in IoT systems,
Zhang, Y. et al. (2017)	Investigate secure communication in IoT	Cryptographic algorithms, simulation	Evaluated the performance and security of different communication protocols (e.g., MQTT, CoAP) in IoT environments
Smith, J. et al. (2018)	Analyze privacy challenges in IoT ecosystems	Literature review, case studies	Identified key privacy challenges in IoT, including data protection, user consent, and device authentication
Chen, W. et al. (2018)	Analyze user-centric privacy control in IoT	User surveys, privacy policy analysis	Identified user preferences and concerns regarding privacy control in IoT devices and proposed user-centric design recommendations
Chen, L. et al. (2019)	Propose a privacy-preserving IoT data aggregation scheme	Cryptographic protocols, simulation	Developed a privacy-preserving data aggregation scheme using homomorphic encryption, ensuring data privacy while allowing for useful analysis
Kim, J. et al. (2019)	Investigate machine learning-based anomaly detection in IoT	Machine learning algorithms, real-world dataset analysis	Developed an anomaly detection framework using machine learning algorithms to detect security breaches and abnormal behaviors in IoT networks
Zhang, H. et al. (2020)	Investigate security threats in IoT networks	Simulation, threat modeling	Identified various security threats in IoT networks, such as spoofing, eavesdropping, and denial-of-service attacks
Li, X. et al. (2021)	Examine the impact of differential privacy in IoT	Experimental evaluation, data analysis	Showed that applying differential privacy techniques to IoT data can provide a balance between privacy protection and data utility
Islam et al. (2021)	Explored the emerging field of edge computing for IoT security and privacy	It highlighted the need for secure edge computing architectures and edge-enabled security	Developed edge computing in reducing latency and enhancing data privacy by processing data closer to

Reference	Research Objective	Methodology	Key Findings
Alaba et al. (2017)	Security measures, including encryption, authentication, and access control mechanisms	comprehensive survey of IoT security and privacy issues.	Identified various threats and vulnerabilities in IoT systems,
		mechanisms.	the source
Lee, S. et al. (2022)	Explore secure firmware update mechanisms for IoT devices	Case studies, analysis of update protocols	Proposed an over-the-air update framework with cryptographic mechanisms to ensure secure and authenticated firmware updates in IoT devices

Table-1 : Literature Survey

IOT SECURITY AND PRIVACY CHALLENGES

IoT brought users huge benefits; however, some challenges come along with it. Cybersecurity and privacy risks are the primary concerns of the researchers and security specialists cited. These two are posing a considerable predicament for many business organizations as well as public organizations. Prevalent high-profile cybersecurity attacks have demonstrated the vulnerabilities of IoT technologies. This vulnerability is simply because the interconnectivity of networks in the Internet of Things brings along accessibility from anonymous and untrusted Internet requiring novel security solutions [13].

Of all the challenges that are known, none of them has a more significant influence on IoT adaptation, such as security and privacy. It is, however, unfortunate that the users do not often have the required acknowledgment of the security impacts until the time when a breach has occurred, causing massive damages such as loss of crucial data. With the ongoing security breaches which have compromised the privacy of users, the appetite of the consumers for poor security is now declining. In a recent review conducted regarding privacy and security, consumer-grade Internet of Things did not do well. There were a lot of vulnerabilities in modern automotive systems.

" The rapid proliferation of Internet of Things (IoT) devices has raised significant concerns regarding privacy and security, creating a pressing need to address the vulnerabilities and risks associated with IoT systems."

IoT (Internet of Things) devices have become increasingly popular in recent years, connecting everyday objects to the internet and enabling communication and data exchange between them. While IoT offers numerous benefits and conveniences, it also presents significant security and privacy challenges. Here are some of the key challenges associated with IoT security and privacy:

- **Vulnerabilities**: Many IoT devices have vulnerabilities in their firmware, software, or communication protocols that can be exploited by hackers. These vulnerabilities can lead to unauthorized access, data breaches, or even control of the device by malicious actors.
- **Lack of standardization:** The IoT ecosystem lacks consistent security and privacy standards. The wide variety of devices from different manufacturers with varying levels of security practices makes it difficult to establish uniform security measures across the board.
- **Weak authentication and authorization:** IoT devices often have weak authentication mechanisms, such as default or easily guessable credentials. Additionally, authorization mechanisms may be inadequate, allowing unauthorized access to device functionalities and data.
- **Data privacy:** IoT devices collect and generate vast amounts of data about users' behaviors, preferences, and even personal information. If this data is not handled and stored securely, it can be vulnerable to unauthorized access, leading to privacy breaches and potential misuse of sensitive information.
- **Inadequate encryption:** Many IoT devices lack proper encryption mechanisms for data transmission and storage. Without encryption, data can be intercepted or tampered with, compromising its confidentiality and integrity.

- **Firmware and software updates:** IoT devices often have long lifecycles, and manufacturers may not provide regular firmware and software updates to address security vulnerabilities. This leaves devices exposed to known exploits for extended periods, making them easy targets for attackers.
- **Physical security:** IoT devices are often deployed in diverse environments, including public spaces and industrial settings. They can be physically tampered with, leading to unauthorized access or manipulation of the device's functions.
- **Interoperability issues:** The interoperability of different IoT devices and platforms can introduce security risks. Integration challenges may arise when devices from different manufacturers with varying security measures need to communicate and share data securely.
- **Lack of user awareness:** Many IoT users are not fully aware of the security and privacy risks associated with these devices. They may not change default passwords, update firmware regularly, or take other necessary precautions, making their devices more susceptible to attacks.
- **Supply chain vulnerabilities:** The complex supply chain involved in manufacturing and distributing IoT devices can introduce security risks. Malicious actors may exploit vulnerabilities at various stages of the supply chain, compromising the integrity and security of the devices.

Addressing these challenges requires a multi-faceted approach involving manufacturers, policymakers, and users. It involves implementing robust security measures in IoT devices, establishing industry-wide security standards, promoting user education and awareness, and ensuring regulatory frameworks are in place to protect user privacy and incentivize manufacturers to prioritize security in their products.

By the development of more advanced security features and building these features into products, hacks may be evaded. This evasion is because the users will buy products that already have proper security features preventing vulnerabilities. Cybersecurity frameworks are some of the measures put forward to ensure that IoT is secure [18].Moreover, some several factors and concerns might have an impact on compromising the efforts to secure the Internet of Things devices; these include:

- **Occasional update:** usually, IoT manufacturers update security patches quarterly. The OS versions and security patches are also upgraded similarly [19]. Therefore, hackers get sufficient time to crack the security protocols and steal sensitive data.
- **Embedded passwords:** IoT devices store embedded passwords, which helps the support technicians to troubleshoot OS problems or install necessary updates remotely. However, hackers could utilize the feature for penetrating device security.
- **Automation:** often, enterprises and end-users utilize the automation property of IoT systems for gathering data or simplifying business activities. However, if the malicious sites are not specified, integrated AI can access such sources, which will allow threats to enter into the system.
- **Remote access:** IoT devices utilize various network protocols for remote access like Wi-Fi, ZigBee, and Z-Wave. Usually, specific restrictions are not mentioned, which can be used to prevent cybercriminals. Therefore, hackers could quickly establish a malicious connection through these remote access protocols.
- **Wide variety of third-party applications:** several software applications are available on the Internet, which can be used by organizations to perform specific operations. However, the authenticity of these applications could not be identified easily. If end-users and employees install or access such applications, the threat agents will automatically enter into the system and corrupt the embedded database.
- **Improper device authentication:** most of the IoT applications do not use authentication services to restrict or limit network threats. Thereby, attackers enter through the door and threaten privacy.
- **Weak Device monitoring:** usually, all the IoT manufacturers configure unique device identifiers to monitor and track devices. However, some manufacturers do not maintain security policy. Therefore, tracking suspicious online activities become quite tricky.

By combining these proposed solutions and leveraging new methods and algorithms, the privacy and security of IoT systems can be significantly enhanced. However, it is crucial to consider the specific requirements and constraints of different IoT use cases and ensure the practicality, scalability, and interoperability of these solutions in real-world deployments.

FUTURE OF THE INTERNET OF THINGS

The future of the Internet of Things (IoT) holds tremendous potential for transforming various aspects of our lives. Here are some key trends and possibilities that can shape the future of IoT:

1. **Expansion of IoT devices:** The number of IoT devices is expected to grow exponentially. We will witness a proliferation of interconnected devices in various domains, including smart homes, healthcare, transportation, agriculture, manufacturing, and cities. This expansion will create a vast network of interconnected objects, enabling seamless data sharing and automation.
2. **Edge computing and processing:** With the growing number of IoT devices generating massive amounts of data, there will be an increased emphasis on edge computing. Edge devices will process and analyze data locally, reducing latency and bandwidth requirements. This distributed computing paradigm will enable faster response times, improved efficiency, and enhanced privacy by keeping sensitive data closer to the source.
3. **Artificial Intelligence (AI) integration:** AI technologies will play a vital role in unlocking the full potential of IoT. AI algorithms will analyze IoT-generated data to extract meaningful insights, detect patterns, and make intelligent decisions. AI-powered IoT systems can optimize processes, enhance automation, and enable predictive capabilities, leading to improved efficiency and personalized experiences.
4. **5G connectivity:** The deployment of 5G networks will revolutionize IoT connectivity. 5G offers ultra-low latency, high bandwidth, and massive device connectivity, making it ideal for IoT applications. It will enable real-time communication, support high-density deployments, and enhance the performance of IoT devices across various industries.
5. **Blockchain for IoT security:** Blockchain technology can provide enhanced security and privacy in IoT deployments. It offers decentralized and tamper-proof data storage, authentication, and secure transactions. Blockchain can ensure the integrity of data collected by IoT devices, enable secure device-to-device communication, and establish trust in IoT ecosystems.
6. **Smart cities and infrastructure:** IoT will play a crucial role in creating smart and sustainable cities. Connected sensors and devices will monitor and optimize various aspects, such as energy consumption, traffic management, waste management, and public safety. Smart infrastructure will enhance the quality of life for citizens, improve resource efficiency, and enable data-driven urban planning.
7. **Environmental monitoring and sustainability:** IoT can help address environmental challenges by monitoring and managing resources efficiently. IoT devices can monitor air quality, water quality, energy usage, and waste management. By analyzing this data, organizations and individuals can make informed decisions to reduce environmental impact and promote sustainability.
8. **Enhanced healthcare and telemedicine:** IoT will revolutionize healthcare by enabling remote patient monitoring, personalized treatment, and preventive care. Wearable devices, smart sensors, and medical implants can continuously monitor vital signs, track health conditions, and transmit data to healthcare professionals in real-time. Telemedicine will become more widespread, enabling remote consultations and improving access to healthcare services.
9. **Industry 4.0 and automation:** IoT will continue to drive the evolution of industries through automation and optimization. Industrial IoT (IIoT) will enable real-time monitoring, predictive maintenance, and intelligent supply chain management. Smart factories will leverage IoT devices, robotics, and AI to enhance productivity, reduce costs, and improve overall efficiency.
10. **Ethical and privacy considerations:** As IoT becomes more prevalent, ethical and privacy concerns will gain prominence. There will be a need for robust data protection regulations, transparency in data usage, and consent mechanisms to ensure user privacy and prevent misuse of personal information.

The future of IoT holds immense possibilities, but it also comes with challenges. Addressing security, privacy, and interoperability concerns, along with developing robust standards and regulations, will be crucial in realizing the full potential of the Internet of Things.

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.
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

In this work, we propose a new view of the IoT models: generic and stretched with the privacy and security components and layers identification and separation. We built a cloud/edge supported IoT system to implement the proposed IoT models. Therefore, in this work we first introduce the generic and stretched models, then describe our experimental setup and implementation environment (layered model implementation), and then present and discuss the results and findings.

Generic IoT Layers and Data Fusion Model

The generic architecture of the IoT model, from the authors' perspective, not sure if there are any similar thoughts in literature, as shown in Figure 1, consists of a device, cloud, and end-user layers. The device layer consists of a pool of wireless Internet-enabled sensor devices, data acquisition circuitry, and communication protocols to send data to local or remote storage for further processing. These devices allow the user to collect data in real-time with different acquisition frequencies. The cloud layer hosts the data collected from the sensors for further processing, noise removal, feature extraction, and data massaging. This data is later fed into a decision support system that runs complex data analysis and artificial intelligence to provide a decision regarding the person's health. The end-user layer, consisting of the receiving user, could be in different forms. Of concern is smart devices, where security and privacy challenges exist. Within the boundaries of these three layers, a list of sublayers or modules added to ensure the robustness of the decision support system. To ensure data is sent and processed promptly to provide a critical decision that cannot wait until the data is sent to the cloud, we introduce an edge computing capability that can make such smart decision, and at the same time save a copy of the data and send it to the cloud layer for processing and long-term storage. On certain occasions, we need to send commands or instructions to some wearables devices to update their acquisition rate or functionality, and this will require another protocol and security procedure.

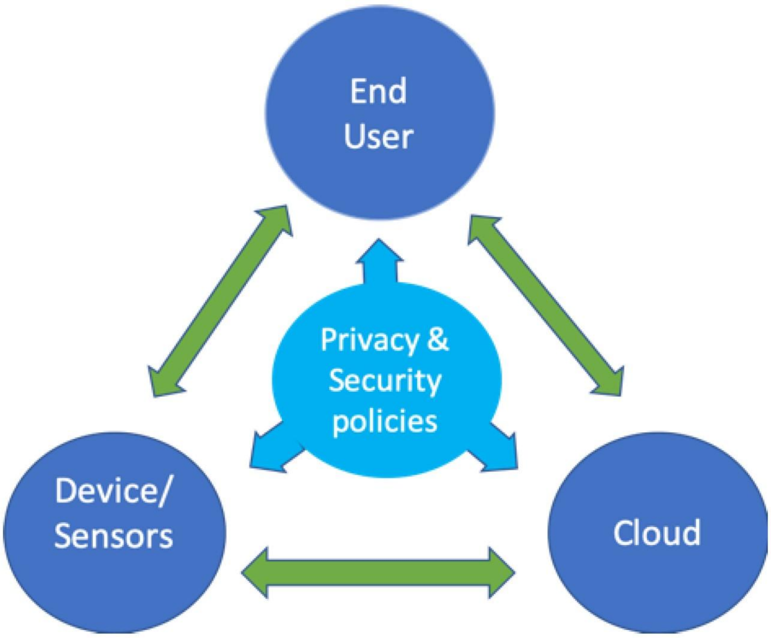

Figure 1. Internet of Things (IoT) generic model with privacy and security policies.

Figure 2 shows the stretched version of the generic model. We can see the addition of the new layers; edge and fog. Both layers can overcome the latency issues from the reliance on cloud layer services and are able to make decisions faster. Edge computing occurs on the devices to which the sensors are attached to or physically close. They provide a real-time decision and control to the data sources, and at the same time, communicate with other layers to transfer the data for fusion, storing, and analytics. The fog computing layer moves the edge computing activities to more powerful computing resources that are connected to the local area network and physically more distant from the sensors and data sources [28]. These added benefits create more security and privacy challenges.

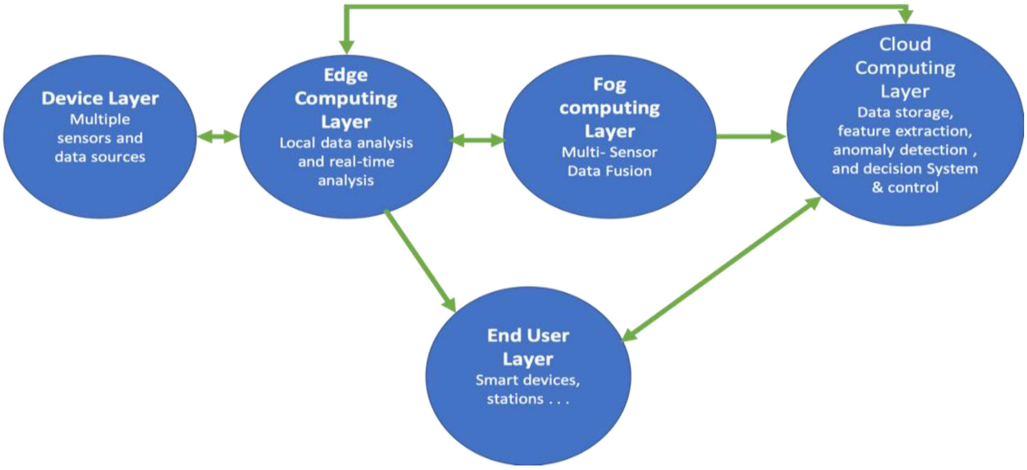
Device Layer
Multiple sensors and data sources
Edge Computing Layer
Local data analysis and real-time analysis
Fog computing Layer
Multi- Sensor Data Fusion
Cloud Computing Layer
Data storage, feature extraction, anomaly detection , and decision System & control
End User Layer
Smart devices, stations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

Figure 2. IoT stretched model.

Security and Privacy Policies

Cloud-based services are often considered as the essential infrastructure of the IoT that provides support for data storage, data processing, and data sharing [29]. Hackers and attackers are targeting IoT computing devices and nodes that store or communicate sensitive data. For example, patient information and electronic medical records make the healthcare system a valuable target for hackers. Each layer of the IoT model introduces security challenges and, at the same time, a possibility to enforce security and privacy standards and protocols. For example, in the device layer, the sensor's data is sent to the edge, fog, and then to the cloud, a need for authorization and certificates that trust specific servers to minimize these attacks. Firmware security and hardware address authenticating and more, however, this comes at the cost of the power consumption, as some of the wireless enabled devices such as wearables are battery run. Such security measures need to be revisited to accomplish both security and power constraints. On the cloud layer, security measures need to ensure the network protocol between the edge and fog nodes and occasionally from sensors. Message passing protocol, point to point encryption, and certificates all provide less data spying and logging. In the data processing and end-user level, we need to ensure that the long-term data storage and real-time data processing are protected from SQL injections, sniffing, and phishing scripting attacks, providing the service certificate is updated and complies with the HIPPA standards (in health systems) [30]. Data fusion can introduce another access to the hackers to identify the user, hence privacy breach. Since the IoT devices can join and leave the network of sensors and data sources, this adds more complication to the standard methods of security measures, hence the need for new intelligent and adaptable security measures [31].

Implementation of the Proposed Layered Cloud-Edge-IoT Model

Our approach is to ensure security measures set before deploying the IoT enabled devices into the secured network and ensure they can securely communicate and share data, to protect the privacy of data through encryption. Figure 3 below shows the abstraction of hardware, software, and communication model. The model consists of AWS cloud as master cloud, Raspberry Pi 4 as Edge Node, and Virtual Machines as IoT devices. The system we created with an AWS paid account to have full access to the resources provided by AWS, including certificate and encryption keys, authorization, and authentication [32].

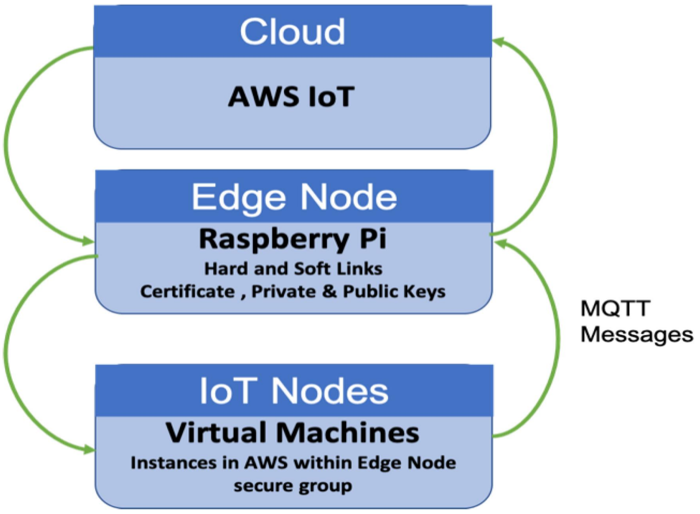

Figure 3. The proposed system model.

The proposed IoT model showed that we could ensure privacy and security measures set before we allowed the IoT enabled device or node to communicate or share its data. Upon successful implementation and configuration, we are sure that our assets are protected. The described model in this paper can be used to provide secure IoT environments and systems with fog/edge computing layers and sensors fusion. Many real-life applications can utilize this model, such as healthcare, military, disaster recovery, and many others [35]. Let us consider the healthcare case; for example, by using the proposed policy-based model, the users will have the ability to trust their healthcare provider to allow them a safeguard so that they know they are looked after. Healthcare companies invest in wearables with the belief they will help improve workforce productivity, cut absenteeism, and reduce healthcare costs. Another significant factor in wearable devices is the conviction that it can give people who are disabled. For example, a person with special needs will be able to input commands and text, say, by just moving a finger up and down. A final method, but not limited to, is the number of security users that could apply to their accounts. For example, people could restrict who can view their social media posts or policies that explain the importance of more security to add to their account (i.e., two-factor authentication) [36].

While the IoT applications (healthcare in this case) developers try to do the best for their customers, there are still some loopholes that tend to fall through. One of the disadvantages would be the way the user's data is stored and how third parties handle it. It mostly relies on the provider itself to ensure that they set guidelines and propose a policy that will keep them in the right with the vendors and with their users. That same thing goes for the confidentiality of the customers. Most of the time, third parties (such as the insurance companies) can receive user's information if they "consent" to it, and then from there, it could be dangerous to determine whether or not it is reliable.

CONCLUSION

In conclusion, ensuring privacy and security in the context of the Internet of Things (IoT) is of paramount importance. The rapid growth of IoT devices has brought numerous benefits but has also introduced significant challenges and risks. This necessitates robust measures and strategies to safeguard user privacy, protect sensitive data, and mitigate security vulnerabilities. Throughout this discussion, we have explored various aspects of IoT privacy and security, including existing methods, algorithms, and proposed solutions. Literature surveys have shed light on the current state of research in this field, highlighting the need for standardized privacy policies, improved authentication mechanisms, secure communication protocols, and continuous firmware updates.

Additionally, we have identified key challenges such as data breaches, lack of standardization, privacy concerns, and scalability issues. These challenges underscore the importance of implementing privacy-preserving techniques, enhancing authentication and access control, addressing firmware vulnerabilities, and promoting user awareness and control over their data. Furthermore, emerging technologies such as blockchain, machine learning, and edge computing hold promise for enhancing IoT privacy and security. Leveraging these technologies, along with novel algorithms and architectures, can strengthen the protection of IoT ecosystems and mitigate the risks associated with unauthorized access, data breaches, and privacy infringements.

To overcome the disadvantages and challenges in IoT privacy and security, collaboration among stakeholders is vital. Manufacturers, developers, policymakers, and end-users must work together to establish industry standards, promote best practices, and raise awareness about the importance of privacy and security in the IoT landscape. By addressing these issues head-on, we can create a safer and more trustworthy IoT environment, fostering innovation while safeguarding user privacy and protecting sensitive data. Only through collective efforts can we unlock the full potential of the IoT while maintaining the privacy and security rights of individuals and organizations.

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).

[31] Thierer, A.D. The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation. 2015. Available online: http://jolt.richmond.edu/v21i2/article6.pdf (accessed on 6 March 2020).

[32] Available online: https://docs.aws.amazon.com/iot/latest/developerguide/what-is-aws-iot.html (accessed on 17 March 2020).

[33] Available online: https://www.tecmint.com/protect-hard-and-symbolic-links-in-centos-rhel/ (accessed on 26 May 2020).

[34] Available online: https://docs.aws.amazon.com/iot/latest/developerg uide/iot-message-broker.html (accessed on 25 May 2020).

[35] Sethi, P.; Sarangi, S. Internet of Things: Architectures, Protocols, and Applications. J. Electr. Comput. Eng. 2017, 1–25. [Google Scholar] [CrossRef][Green Version]

[36] Liyanage, M.; Braeken, A.; Kumar, P.; Ylianttila, M. IoT Security: Advances in Authentication; John Wiley & Sons: West Sussex, UK, 2020. [Google Scholar]