RESEARCHERID
THOMSON REUTERS

[Gopinath, 5(4): April 2018]

ISSN 2348 – 8034
Impact Factor- 5.070

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

SECURITY AND PRIVACY CHALLENGES IN IOT NETWORKS

Dr. Madhu Gopinath
Designation: Associate professor
Email: madhugopinath.bsfit@gmail.com
Institute: Border Security Force institute of technology

ABSTRACT

The Internet of Things (IoT) revolutionized today's connectivity by connecting billions of intelligent devices across industries like healthcare, education, and business. But this innovation comes with massive security and privacy issues as a result of the heterogeneity, scalability, and physical exposure of IoT devices. This paper discusses the evolution, uses, and in-built threats of IoT, with special emphasis on challenges including no standardization, device visibility, unsecure data transmission, botnet threats, and ransomware attacks. An evaluation of the literature identifies other solutions in the form of homomorphic encryption, blockchain, and quantum-enhanced cryptography. To tackle these issues, the paper suggests a cloud-edge-IoT layered architecture on AWS, Raspberry Pi, and virtual machines. The framework stresses secure encryption, authentication, and access controls by leveraging secure MQTT-based communication and AWS Greengrass Core. The deployment validates the practicability of secure, scalable, and efficient IoT systems by guaranteeing privacy before data sharing. This model enables real-time processing with security, which makes it appropriate for critical applications such as healthcare and disaster relief. Finally, this work helps in creating best practices and policies for protecting data in IoT networks.

Keywords*: IoT, MQTT, Raspberry Pi, AWS.*

I. INTRODUCTION

The Internet has brought remarkable communication and network infrastructure, which profoundly affects society and the economy. Its frequency has increased with the emergence of affordable wireless connections [1]. New technology has enabled billions of people to access the web via their smartphones, tablets, and laptops. Following this phase, the next major development is enabling networked computers to share data with interconnected things [2]. The IoT is a component of the future Internet that will include billions of "things" that can communicate intelligently. There is a seemingly endless list of goods that might be upgraded shortly, including books, vehicles, electrical appliances, food, water heaters, intelligent buildings, and even shoes [3]. Products that formerly included just mechanical and electrical components will revert to including hardware, sensors, electronics, and intricate gadgets networked in various formats over the internet and certain platforms [4].

As the information and communication technology revolution of the 21st century continues, a new platform known as the IoT has arisen. Education, healthcare, commerce, the public sector, and numerous governmental entities are among the many fields that make use of this platform to provide resources and services on demand [5]. The IoT is a revolutionary concept that will allow the physical and digital worlds to merge. The IoT is a network architecture that communicates across the real and virtual worlds via the interconnection of everyday physical items [6].

ISSN 2348 – 8034
Impact Factor- 5.070

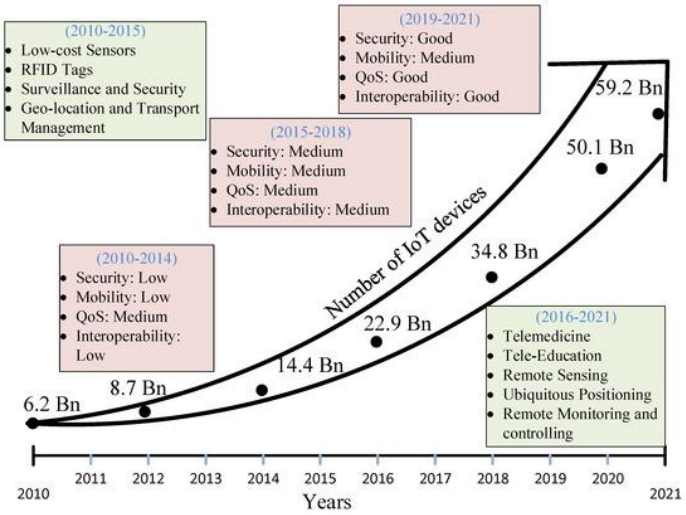

Figure 1: IoT Evolution [7].

The IoT is a new paradigm in the context of contemporary wireless communications that is quickly becoming popular [8]. "Radio-Frequency Identification (RFID)" tags, actuators, sensors, mobile phones, etc., are just a few examples of the common things that can interact with one another and work together to accomplish common goals due to their unique addressing schemes [9]. The term IoT was primary used by "Kevin Ashton in 1999" during a presentation for Procter & Gamble Company. It organized and advocated for the advantages of using RFID technology in the supply chain, leading to its widespread recognition via the Auto-ID Centre at MIT [11]. The idea of the IoT was subsequently recognized by academics and scientists. A formal definition of the IoT was provided in 2005 by the International Telecommunications Union (ITU). ITU published a study online under the title "IoT" [12].

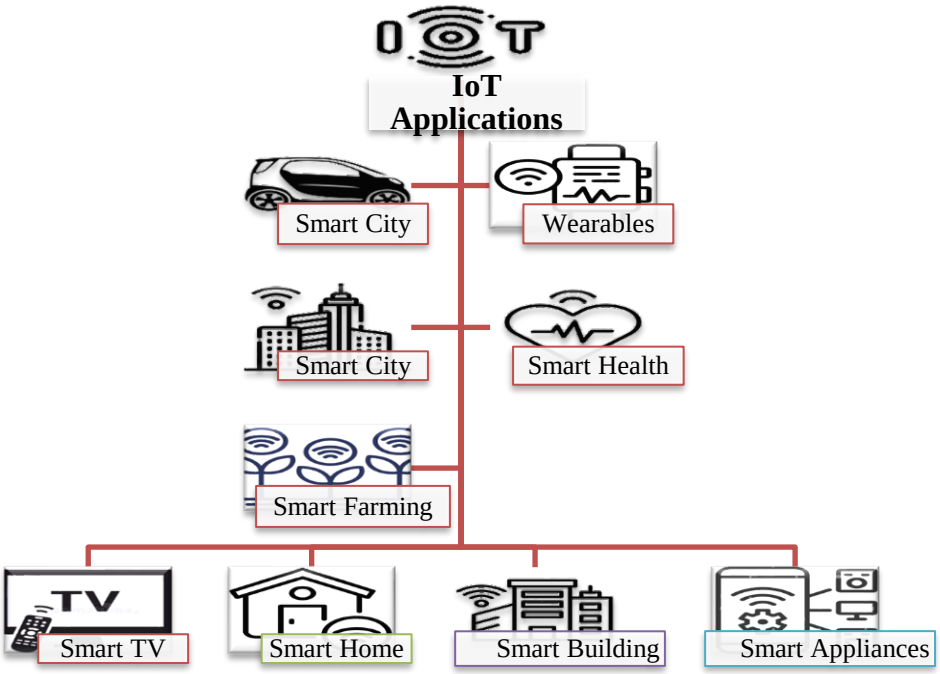

Figure 2: Application of IoT [13].

Daily, new technologies are introduced or modifications are implemented to old ones. In this regard, think about the recent growths in the 5G network. There is a strong expectation that 5G will be pivotal in the development of IoT systems and apps. Concerns about privacy and security due to its high frequency and bandwidth have drawn the curiosity of researchers. The short wavelength, however, necessitates infrastructure upgrades in the form of more base stations to cover the same region as competing wireless technologies. Additional dangers, such as phony base stations, are introduced by this reorganized system. Researchers must be well-versed in the security dangers and possible remedies.

The study determines to observe the uses, advantages, and possible dangers of the IoT. Further goals include creating a structure for research regarding and improvement of optimal security practices by analysis of existing schemes, their implementation, or the creation of new ones. The results inform the suggestions for mitigating these risks and addressing any potential security vulnerabilities. The study will help stakeholders in the IoT create and implement better security and privacy safeguards, as well as regulatory authorities in their policy enforcement efforts.

Researchers used a narrative review approach to delve into the context of IoT systems, their development, privacy and security concerns, and the solutions to these problems. Concerning the general and expanded IoT paradigm, they put forward the perspective on the subject of privacy and security. Researchers constructed and investigated an IoT model that made use of cloud services (AWS), edge nodes (Raspberry Pi), and virtual machines (sensors).

1.1 IoT Security Challenges

IoT initiates a transformation in connection, facilitating seamless communication across devices. However, this enhanced interdependence presents several security issues. Figure 2 illustrates many critical security problems related to the IoT.

Figure 3: IoT Security Challenges

- **Lack of Physical Security**

IoT devices are susceptible to illegal access because they lack strong physical protections. Particularly vulnerable to manipulation are devices left in remote areas for long periods of time. A major security concern is the simplicity with which attackers can target IoT devices that have no physical protection [14,15].

- **Lack of Standardization**

The IoT is made by an extensive variety of companies, each of which uses its own set of standards and protocols. Vulnerabilities, giving possible access points for exploitation, might result from the lack of standardized security measures.

It is already difficult to build a unified security architecture for the IoT due to the discordance in manufacturing procedures and standards. It becomes tough to ensure compatibility and security across the board because devices could communicate differently and prioritize varying security elements [16].

- **Lack of Visibility**

It is already difficult to build a unified security architecture for the IoT due to the discordance in manufacturing procedures and standards. It becomes tough to ensure compatibility and security across the board because devices could communicate differently and prioritize varying security elements [16].

- **Data Privacy and Integrity**

Data privacy has become a critical issue in the realm of IoT security. From smart toys and wearables that leak personal information to medical equipment that divulges patient details, user data flows across multiple gadgets. An example of this would be a cybercriminal stealing sensitive company data and then either selling it or using it as leverage to blackmail the owner [19].

- **Physical Security Threats**

IoT devices are susceptible to direct manipulation and interference due to their physical nature. Attackers could compromise these devices by physically accessing their hardware, which gives them the ability to change their functionality or steal critical data. This real-world component of the IoT highlights the need for physical and digital security measures to prevent intrusions [20].

- **Insecure Data Storage and Transmission**

Most IoT devices don't encrypt data at rest or in transit. Because of this carelessness, the data is vulnerable to surveillance and other forms of unjustified access. These inadequate security measures highlight the critical need for stronger encryption algorithms in the IoT environment to prevent breaches and unwanted intrusions [21,22].

- **Botnet Attacks**

A major security concern about IoT directly involves the devices themselves. Their intrinsic security weaknesses make them great candidates for botnet intrusions. A botnet is a collection of devices infected by software. Perpetrators use these exploited systems to inundate targets with excessive request volume [23,24].

- **Ransomware**

Ransomware encrypts and blocks access to critical data, making it a major threat to IoT security. To get back in, hackers usually ask for money, or a ransom, in return for the key to decrypt [25]. Although it is rare at the moment, ransomware might infect IoT devices with inadequate protection in the future. Due to their crucial relevance to users, healthcare equipment, smart homes, and other intelligent products could become more appealing targets as their value and reliance increase [26].

II. LITERATURE REVIEW

The convergence of Cloud Computing with the IoT, or the Cloud of Things (CoT), has revolutionized pervasive computing while at the same time generating serious safety and privacy concerns due to the use of common distant resources and high data processing needs [27]. These worries echo through the larger IoT ecosystem, where the proliferation of connected devices generates needs for strong security practices, particularly those that counter threats at each protocol layer [28]. As IoT systems become used across a wide range of sectors such as healthcare, industry, and infrastructure, their reliance on embedded devices capturing and transmitting sensitive data raises fears of device surveillance, poor upgrade processes, and poor security practices [29]. To counter these, advanced encryption methods such as Key Policy Attribute-Based Encryption (KP-ABE) have been created; however, their requirement for high resources has also generated more resource-efficient quantum-enhanced versions [30].

In addition, since multimedia information such as audio, video, and images are typically exchanged through IoT devices, secure key management and methods such as blockchain and quantum encryption are being investigated to improve data privacy and inhibit unauthorized access [31]. Homomorphic encryption has also been suggested for secure IoT system communication with consideration of reducing encryption overhead while ensuring privacy in data storage and transmission levels, especially in optical fiber communications [32]. IoT's extensive deployment inside smart cities, industries, and services such as healthcare underscores its efficiency advantages but poses security threats due to system and data streams heterogeneity [33]. As countermeasure against centralized threats, blockchain has been suggested in IoT systems to facilitate decentralized authentication and secure data exchange, reducing attacks such as device spoofing and imitation data injection while ensuring transparency and robustness across applications [34]. Overall, these studies underscore the interrelated nature of IoT security threats and the continuous exploration of encryption, cloud integration, and blockchain mechanisms to mitigate them.

ISSN 2348 – 8034
Impact Factor- 5.070

III. PROPOSED IOT LAYERED MODELS

The study presents a new perspective on IoT models, one that is both general and expanded to include privacy and security features, as well as additional identification and separation levels. To put these IoT models into action, researchers developed a cloud/edge-supported IoT solution. Following an introduction to the generic and stretched models, the study details the experimental setup and implementation environment.

1.2 Data Fusion Model and Generic IoT Layers

Figure 4 shows the three levels of the general IoT architecture: device, cloud, and end-user. The device layer enables the network of Internet-connected, wireless sensor devices to acquire data in real time at various frequencies using communication protocols and data collection circuits. Processing of the data is then sent to either local or distant storage. The cloud layer performs storage, noise reduction, feature extraction, and data preparation that is used by a decision support system based on advanced analytics and AI to determine an individual's health status. The end-user layer includes users using the system, typically via smart devices, which brings privacy and security issues into focus. To support responsiveness, an edge computing feature is built to enable real-time decision-making if important data is not available to wait for processing in the cloud. It also streams data to the cloud for future use. The system also enables sending commands to wearable devices—like changing acquisition rates—which needs specialty communication protocols and secure processes. This multi-layered construct, made possible by modular components, provides a secure, responsive, and robust IoT framework for health-decision-making.

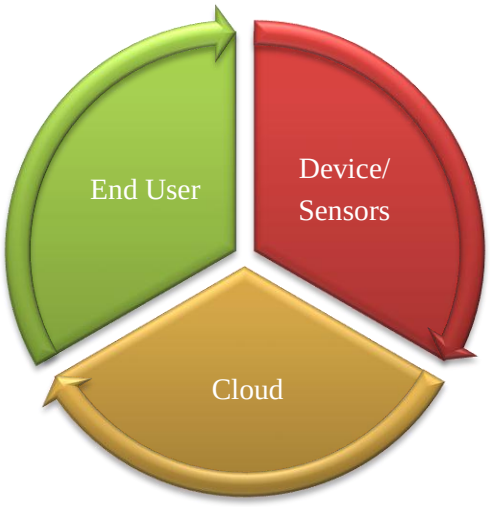

Figure 4: Generic IoT model

The newly added layers of edge and fog are visible. By eliminating the need for cloud-based services, both levels can make quicker judgments and avoid the latency problems that come with them. The devices that the sensors are physically near or connected to are where the edge computing takes place. The data sources are controlled, and choices are made in real time by these layers, which also interact with each other to transmit data for analytics, storage, and fusion. The fog computing layer offloads computations typically done at the network's periphery to servers located further absent from the original data sources and sensors but still connected to the local area network [35].

1.3 The Suggested Layered Cloud-Edge-IoT Architecture

Protecting data privacy via encryption is the priority; therefore, researchers take precautions before putting IoT-enabled devices into a safe network and make sure they can link and conversation data safely. The model's abstraction of the software, hardware, and communication components is shown in Figure 5. The AWS cloud serves as the main cloud in this paradigm, while Virtual Machines and “Raspberry Pi 4” serve as the edge nodes and IoT devices, respectively. Full access to all AWS resources, such as authorization, certificates, encryption keys, and authentication, was granted at system creation using an AWS premium account.

ISSN 2348 – 8034
Impact Factor- 5.070

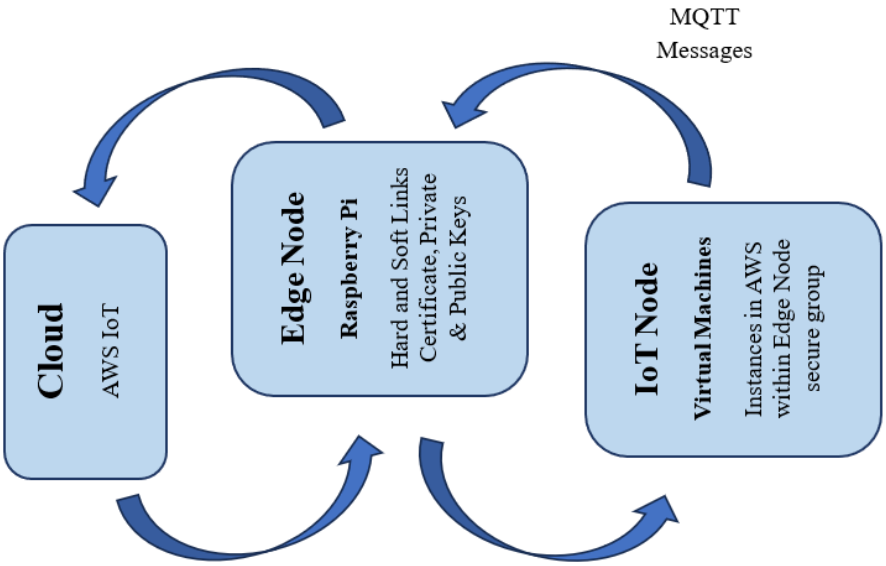

Figure 5: The proposed system model

Researchers used the "AWS Identity and Access Management (IAM)" web service from the accessible AWS resources. It enabled us to regulate user access by establishing an IAM account for each individual. For safety reasons, they refrained from using the AWS Root account and instead created an IAM user with administrative privileges. To set up the "R"aspberry Pi" as an AWS Greengrass Core edge node, the Core communicates with the cloud directly and operates locally. To secure the Raspberry Pi, Linux's hard and soft link protection capabilities were installed. So that the Raspberry Pi and AWS could interact with one another. The authors set up a group with an AWS Greengrass Core device as the hub and then added all the other IoT devices so they could talk to the edge.

All devices must be authenticated with AWS, which requires certificates. It establishes a safe linking between the edge and AWS by generating records and private and public keys. After they formed the Greengrass group, AWS produced the core certificates (see Figure 6 below). After getting the files prepared, they launched Greengrass Core on the "Raspberry Pi".

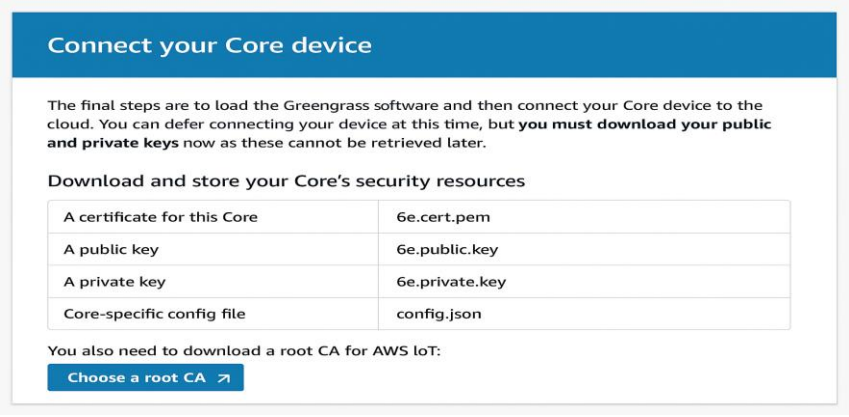

Figure 6: Private, certificate, and public keys.

Examination and Discussion

Researchers created a basic situation in which two IoT-enabled devices interact with each other via the edge infrastructure. The IoT devices were established as virtual computers on AWS and included in the "Greengrass core (GC)", as seen in Figure 7. To authenticate devices with AWS and the GC device, an exclusive certificate and

ISSN 2348 – 8034
Impact Factor- 5.070

private/public keys are issued for every device during the formation process. A message broker, a safe method using the "MQTT protocol", allowed these two devices to communicate with each other. Figure 8 concludes that the data exchanges and successful communication between the IoT nodes and the Edge node were accomplished at the specified timeframes.

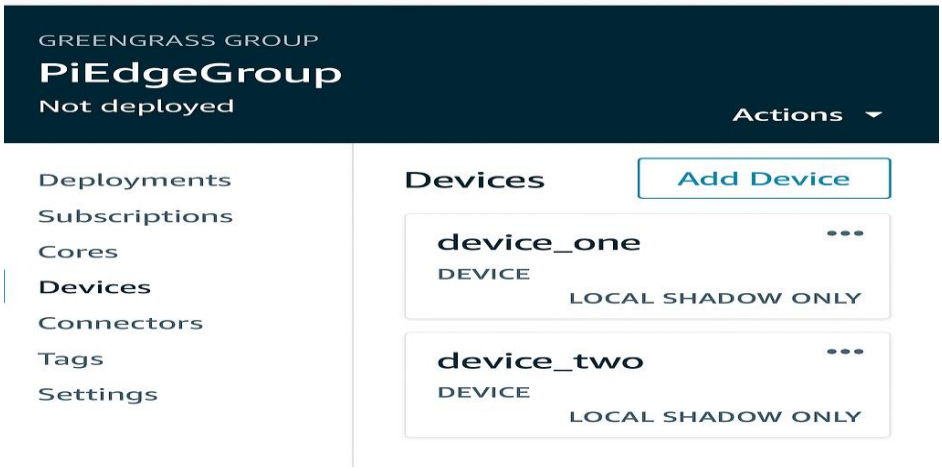

Figure 7: IoT-enabled nodes

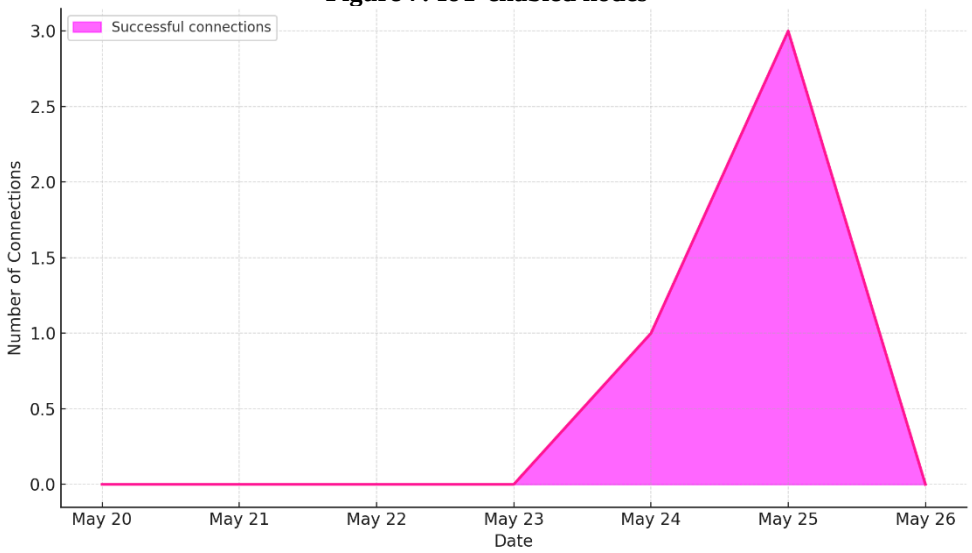

Figure 8: Successful communication among nodes.

Here are the key things to note about the AWS work environment and the methodology researchers used:

- The general model has IoT devices connecting to the cloud through Amazon Web Services IoT Core.
- The model incorporates the edge concept, which is based on AWS's GC IoT core concept and is represented using Raspberry Pi. This allows us to conceptualize it as an extra mediator among the IoT devices, AWS IoT Core, and the cloud.
- The CA Root certificate, which is the AWS IoT certificate, as well as the private key needed by every device individually. A variety of CA Root certificates are available for use with various kinds of IoT devices.
- A policy is required for every device; it specifies the actions the device is allowed to do, such as connect, receive, publish, subscribe, and so on.

ISSN 2348 – 8034
Impact Factor- 5.070

Consequently, researchers developed a certificate, policy, and device. They proceeded by attaching the policy to the certificate, which was then secured to the device. Figure 9 below shows a default policy:

Figure 9: Defaulting device policy in AWS

Figure 10 displays the updated policy for the model. The "machine-to-machine (MQTT)" protocol is used for communication in this case. For real-world applications, such as sensors, MQTT is ideal because of its tiny messages and low power requirements, making it ideal for environments with constraints.

Figure 10: Updated device policy to comprise the suggested model's edge layer.

Figure 11 illustrates the many categories of communications sent throughout a single day. The connection duration is influenced by several variables, including network latency and the platform used.

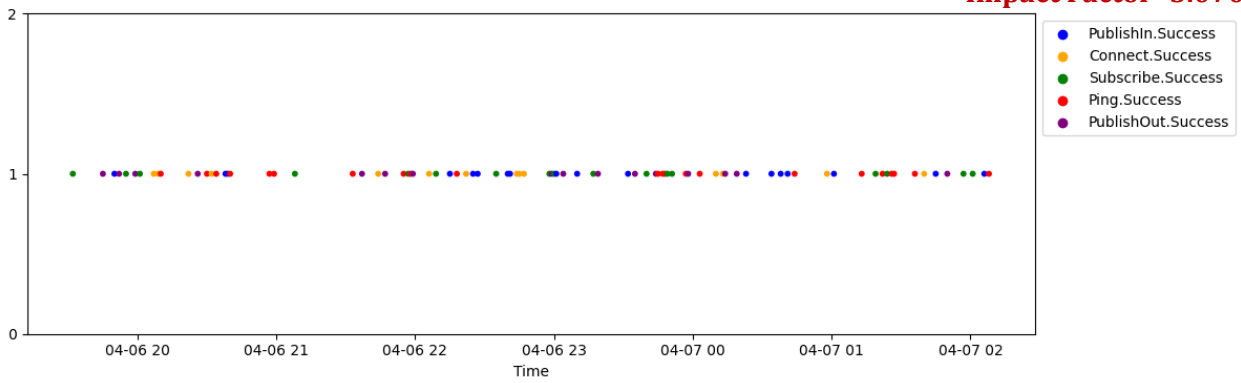

Figure 11: Successfully exchanged messages of different types: Publish Out Success, Publish-In Success, Connect Success, Ping Success, Subscribe Success.

They were able to guarantee the privacy and security safeguards established before granting the IoT-enabled device or node permission to interact or exchange its data, according to the suggested IoT model. Once everything is set up and running well, they will know that the valuables are safe. With the concept outlined in the work, fog/edge computing layers and sensor fusion could potentially be used to create secure IoT environments and systems. The healthcare, military, and disaster recovery industries are just a few examples of the numerous real-world contexts that might benefit from this concept [36].

IV. CONCLUSION

The research identifies growing importance of IoT technologies with particular focus on pressing security and privacy issues that come with them. As IoT gadgets become more enmeshed within everyday life across industries such as healthcare, manufacturing, and smart infrastructure, vulnerabilities to data leakages, unlawful access, and malicious intrusion also grow with compromised physical security, non-standardization, and unprotected data transfer. The research presents a layered IoT model that integrates cloud, edge, and fog computing to mitigate these vulnerabilities. With the integration of AWS cloud services, Raspberry Pi-based edge nodes, and secure communication protocols such as MQTT, the proposed model exhibits a solid framework for securing data exchange and device authentication.

By practical deployment on AWS Greengrass and certificate-based authentication, the work demonstrates efficient techniques for IoT ecosystem security. Granular control of communication is achieved through custom device policies and encryption methods, thereby making the infrastructure more resilient. Fog and edge computing reduce latency and enable real-time decision-making while maintaining data integrity and confidentiality. In the end, this research provides practical insights into the design of secure, scalable IoT systems and delivers a feasible strategy for regulatory bodies and developers looking to enforce and deploy robust privacy and security policies in future IoT installations.

REFERENCE

1. Chandrakanth, S., K. Venkatesh, J. Uma Mahesh, and K. V. Naganjaneyulu. "Internet of things." *International Journal of Innovations & Advancement in Computer Science* 3, no. 8 (2014): 16-20.
2. Kutup, Nejat. "Nesnelerin interneti; 4H her yerden, herkesle, her zaman, her nesne ile bağlantı." *XVI. Türkiye'de İnternet Konferansı* 11 (2011): 151-156.
3. Aktaş, Faruk, Celal Çeken, and Yunus Emre Erdemli. "Nesnelerin interneti teknolojisinin biyomedikal alanındaki uygulamaları." *Düzce Üniversitesi Bilim ve Teknoloji Dergisi* 4, no. 1 (2016): 37-54.
4. Li, Shancang, Li Da Xu, and Shanshan Zhao. "The internet of things: a survey." *Information systems frontiers* 17 (2015): 243-259.
5. Younas, Muhammad, Irfan Awan, and Antonio Pescape. "Internet of things and cloud services." *Future Generation Computer Systems* 56, no. C (2016): 605-606.
6. Erguler, Imran. "A potential weakness in RFID-based Internet-of-things systems." *Pervasive and Mobile Computing* 20 (2015): 115-126.

7. Abid, Muhammad Aneeq, Naokhaiz Afaqui, Muazzam A. Khan, Muhammad Waseem Akhtar, Asad Waqar Malik, Arslan Munir, Jawad Ahmad, and Balawal Shabir. "Evolution towards smart and software-defined internet of things." *AI* 3, no. 1 (2022): 100-123.
8. Paksoy, Turan, İsmail Karaoğlan, Hadi Gökçen, Panos M. Pardalos, and Belkıs TORĞUL. "An experimental research on closed loop supply chain management with internet of things." *Journal of Economics Bibliography* 3, no. 1S (2016): 1-20.
9. Dijkman, Remco M., Bram Sprenkels, Thijs Peeters, and Alexandre Janssen. "Business models for the Internet of Things." *International Journal of Information Management* 35, no. 6 (2015): 672-678.
10. Kadlec, Jaroslav, Radek Kuchta, Radovan Novotný, and Ondřej Čožík. "RFID Modular system for the Internet of Things (IoT)." *Industrial Engineering & Management* 3, no. 4 (2014): 1-7.
11. Gubbi, Jayavardhana, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. "Internet of Things (IoT): A vision, architectural elements, and future directions." *Future generation computer systems* 29, no. 7 (2013): 1645-1660.
12. Tao, Fei, Yiwen Wang, Ying Zuo, Haidong Yang, and Meng Zhang. "Internet of Things in product life-cycle energy management." *Journal of Industrial Information Integration* 1 (2016): 26-39.
13. Singh, Prabhjot. "Cross-layer design for Internet of Things (IoT)-issues and possible solutions." *Dep. Syst. Comput. Eng* (2018): 1-10.
14. Ali, Bako, and Ali Ismail Awad. "Cyber and physical security vulnerability assessment for IoT-based smart homes." *sensors* 18, no. 3 (2018): 817.
15. Attkan, Ankit, and Virender Ranga. "Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence based key-security." *Complex & Intelligent Systems* 8, no. 4 (2022): 3559-3591.
16. Frustaci, Mario, Pasquale Pace, and Gianluca Aloi. "Securing the IoT world: Issues and perspectives." In *2017 IEEE Conference on Standards for Communications and Networking (CSCN)*, pp. 246-251. IEEE, 2017.
17. Ahmed, Shehzad, Tahera Kalsoom, Naeem Ramzan, Zeeshan Pervez, Muhammad Azmat, Bassam Zeb, and Masood Ur Rehman. "Towards supply chain visibility using internet of things: A dyadic analysis review." *Sensors* 21, no. 12 (2021): 4158.
18. Kothari, Sneha S., Simran V. Jain, and Abhishek Venkteshwar. "The impact of IOT in supply chain management." *Int. Res. J. Eng. Technol* 5, no. 08 (2018): 257-259.
19. Wang, Tian, Md Zakirul Alam Bhuiyan, Guojun Wang, Lianyong Qi, Jie Wu, and Thaier Hayajneh. "Preserving balance between privacy and data integrity in edge-assisted Internet of Things." *IEEE Internet of Things Journal* 7, no. 4 (2019): 2679-2689.
20. Kim, Taesic, Justin Ochoa, Tasnimun Faika, H. Alan Mantooth, Jia Di, Qinghua Li, and Young Lee. "An overview of cyber-physical security of battery management systems and adoption of blockchain technology." *IEEE Journal of Emerging and Selected Topics in Power Electronics* 10, no. 1 (2020): 1270-1281.
21. Zhang, Lejun, Minghui Peng, Weizheng Wang, Zilong Jin, Yansen Su, and Huiling Chen. "Secure and efficient data storage and sharing scheme for blockchain-based mobile-edge computing." *Transactions on Emerging Telecommunications Technologies* 32, no. 10 (2021): e4315.
22. Khalaf, Osamah Ibrahim, and Ghaida Muttashar Abdulsahib. "Optimized dynamic storage of data (ODSD) in IoT based on blockchain for wireless sensor networks." *Peer-to-Peer Networking and Applications* 14, no. 5 (2021): 2858-2873.
23. Injadat, MohammadNoor, Abdallah Moubayed, and Abdallah Shami. "Detecting botnet attacks in IoT environments: An optimized machine learning approach." In *2020 32nd International Conference on Microelectronics (ICM)*, pp. 1-4. IEEE, 2020.
24. Ali, Ihsan, Abdelmuttlib Ibrahim Abdalla Ahmed, Ahmad Almogren, Muhammad Ahsan Raza, Syed Attique Shah, Anwar Khan, and Abdullah Gani. "Systematic literature review on IoT-based botnet attack." *IEEE access* 8 (2020): 212220-212232.
25. Humayun, Mamoona, N. Zaman Jhanjhi, Ahmed Alsayat, and Vasaki Ponnusamy. "Internet of things and ransomware: Evolution, mitigation and prevention." *Egyptian Informatics Journal* 22, no. 1 (2021): 105-117.

26. Zahra, Syed Rameem, and Mohammad Ahsan Chishti. "Ransomware and internet of things: A new security nightmare." In *2019 9th international conference on cloud computing, data science & engineering (confluence)*, pp. 551-555. IEEE, 2019.
27. Abba Ari, Ado Adamou, Olga Kengni Ngangmo, Chafiq Titouna, Ousmane Thiare, Alidou Mohamadou, and Abdelhak Mourad Gueroui. "Enabling privacy and security in Cloud of Things: Architecture, applications, security & privacy challenges." *Applied Computing and Informatics* 20, no. 1/2 (2024): 119-141.
28. Mohammad, Nur, Rabeya Khatoon, Sadia Islam Nilima, Jahanara Akter, Md Kamruzzaman, and Hasan Mahmud Sozib. "Ensuring Security and Privacy in the Internet of Things: Challenges and Solutions." *Journal of Computer and Communications* 12, no. 8 (2024): 257-277.
29. Kathole, Atul B., Vinod V. Kimbahune, Sonali D. Patil, Avinash P. Jadhav, and Kapil N. Vhatkar. "Challenges and key issues in IoT privacy and security." In *Communication Technologies and Security Challenges in IoT: Present and Future*, pp. 37-50. Singapore: Springer Nature Singapore, 2024.
30. Singamaneni, Kranthi Kumar, Anil Kumar Budati, and Thulasi Bikku. "An efficient Q-KPABE framework to enhance cloud-based IoT security and privacy." *Wireless Personal Communications* (2024): 1-29.
31. Harinath, Depavath, Madhu Bandi, Archana Patil, M. R. Murthy, and A. V. S. Raju. "Enhanced Data Security and Privacy in IoT devices using Blockchain Technology and Quantum Cryptography." *Journal of Systems Engineering and Electronics (ISSN NO: 1671-1793)* 34, no. 6 (2024).
32. Alqahtani, Abdulrahman Saad, Youssef Trabelsi, P. Ezhilarasi, R. Krishnamoorthy, S. Lakshmisridevi, and S. Shargunam. "Homomorphic encryption algorithm providing security and privacy for IoT with optical fiber communication." *Optical and Quantum Electronics* 56, no. 3 (2024): 487.
33. Singhai, Richa, and Rama Sushil. "An investigation of various security and privacy issues in Internet of Things." *Materials Today: Proceedings* 80 (2023): 3393-3397.
34. Ruan, Zhengping. "Blockchain technology for security issues and challenges in IoT." In *2023 International Conference on Computer Simulation and Modeling, Information Security (CSMIS)*, pp. 572-580. IEEE, 2023.
35. Sohal, Amandeep Singh, Rajinder Sandhu, Sandeep K. Sood, and Victor Chang. "A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments." *Computers & Security* 74 (2018): 340-354.
36. Sethi, Pallavi, and Smruti R. Sarangi. "Internet of things: architectures, protocols, and applications." *Journal of electrical and computer engineering* 2017, no. 1 (2017): 9324035.