https://africanjournalofbiomedicalresearch.com/index.php/AJBR
Afr. J. Biomed. Res. Vol. 27 (October 2024); 886-894

Research Article

Iot and Cybersecurity: Addressing Emerging Threats Through Innovative Computer Science Solutions

Dr. S.Sarojini Devi[1*], Dr. K .N.S . Lakshmi[2], Dr. G.V. Sam Kumar[3], Ms. Uma P[4], Divya Lalita Sri Jalligampala[5], Dr. Venkateswara Rao Gera[6]

[1]Associate Professor in CSE Department, NSRIT Autonomous university Sontyam, Visakhapatnam, Affiliated to JNTU, Vijayanagaram, Email: sarojinidevi.cse@nsrit.edu.in*
[2]Professor in CSE Department, Sanketika Vidya Parishad Engineering College, P.M Palem Visakhapatnam Affiliated to Andhra University, Personal mail_id mnslakshmi.vvit@gmail.com
[3]Associate Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India. gvsamkumar@gmail.com
[4]Assistant Professor, Department of Computer Science, New horizon college, Kasturinagar, Bangalore Mail id rainbow.uma@gmail.com
[5]Assistant professor, CSE Department, Aditya College of Engineering & Technology, Surampalem, Andhra Pradesh, INDIA, lalitha517@gmail.com
[6]Professor, Department of CSE, Kallam Haranadhareddy Institute of Technology, Chowdavaram, Guntur, Andhra Pradesh,INDIA gvraocse777@gmail.com

Abstract
Increased usage of smart devices especially under the internet of things (IoT) have provoked emergence of different security issues as a result of connected devices worldwide. This review article aspires to assess more recent threats on IoT ecosystems and present cutting edge computer science solutions towards these threats. AI, ML, Blockchain, and Quantum Cryptography are discussed for their applicability towards improving the security of the IoT technology. The article also looks at the existing architectures and standard technologies including; Lightweight Machine-Type Communications (LwM2M) as well as Datagram Transport Layer Security (DTLS) as well as the use of cloud and edge computing in the defense against IoT threats. Real-world application examples, smart city and building infrastructure, smart healthcare and industrial IoT use cases provide a use case of these solutions. Finally, the review summarizes future trends and directions of IoT cybersecurity that has presented the significance of continuous research toward standardized, quantized, and privacy-preserving security frameworks.

Keywords: Internet of Things (IoT), Cybersecurity, Artificial Intelligence (AI), Machine Learning (ML), Blockchain, Quantum Cryptography, IoT Security Protocols.

***Author for correspondence:** Dr. S. Sarojini Devi, *Email: sarojinidevi.cse@nsrit.edu.in*

Received: 08/08/2024 Accepted: 11/09/2024

DOI: https://doi.org/10.53555/AJBR.v27i3.3044

Introduction

Internet of Things (IoT) as an innovative idea that interconnects billions of devices throughout the whole world including light switches and home appliances, wearables, industrial and medical devices. There are more than 15 billion IoT device connections throughout the world as of 2023, based on estimations, the number of IoT device connections will surpass 25 billion by 2030. The IoT devices have expanded so many fields including the health sector, production sector, transportation sector and many others while forming a new network of connected devices that enables easy exchange of data in automated manner (Gubbi *et al.,* 2013).

Reaching out to the several advantages of the IoT networks, there has also been major concerns with the cybersecurity issues. Due to the combined connectivity of the IoT devices, these devices are much at risk of different cyber threats such as data leakage, unauthorized control, Distributed Denial of Service (DDoS) attacks and malware (Kolias *et al.,* 2017). For instance, in 2016 a botnet attack referred to as Mirai exploited vulnerabilities on IoT devices and significantly impacted service provision rendering tens of millions of dollars in losses (Antonakakis *et al.,* 2017). Such incidences call for proper measures and strategies to be taken in preventing and protecting the Iot structure and the data it handles.

Another issue for IoT environments is that it contains a large number of different devices and protocols, communication standards, which in turn increases the complexity of the cybersecurity problem. The more or less conventional security measures cannot suffice to spate of IoT networks; hence, stimulating techniques particular to IoT needs (Sicari *et al.,* 2015). New technologies in Computer Science like Artificial Intelligence (AI), Block Chain and Quantum Cryptography provides a hope to make IoT systems secure (Mosenia & Jha, 2016).

In this review, the authors propose to analyze the current state of IoT cybersecurity, consider new threats, and describe fresh solutions that the sphere of computer science offers to deal with them. Hence, the article under review, based on the literature analysis and case studies, presents suggestions about the future developments of the IoT security and valuable advice to researchers and practitioners in the field.

Understanding IoT: A Rapidly Expanding Digital Ecosystem

Internet of Things also known as IoT is described as a connection made between devices that convey and share information through out the internet. These may be as basic as sensors and motors and as sophisticated as smart house appliances, industrial automation, self-driven cars and many more (Xu, He, & Li, 2014). IoT has become a very essential and one of the most significant drivers of digital transformation where industries are adopting new ways of automations, data analysis and decision making (Atzori, Iera, & Morabito, 2010).

Definition and Components of IoT

As noted in several studies, IoT can be described as a system of interconnected tangible objects or “things” that are equipped with sensors, software or other technologies for creating, exchanging and consuming data over the internet (Madakam *et al.,* 2015). These objects can include consumer gadgets that are prevalent in today’s society, for example, fitness wearables and smart home appliances, advanced applications which may involve the use of devices to monitor crop conditions or conditions of a patient far from the clinician’s reach among others (Miorandi *et al.,* 2012). The basic parts of IoT are devices comprising of sensors and actuators, communication channel which can be Wi-Fi, Bluetooth, Zigbee and so on, storage such as cloud computing and processing components such as the edge and fog computing.

Applications and Use Cases Across Various Industries

The use of IoT is numerous, thus cuts across many industries and sectors. In many fields, IoT is used to monitor the patients away from the healthcare center, offer individual treatment strategies, and organize the chronic diseases’ management, which has had positive impacts on the patients (Islam *et al.,* 2015). In manufacturing the adoption of IoT in industrial context, referred to as the Industrial IoT or IIot, has pushed efficiency in production, prognosis of equipment failure without downtime and supply chain optimization (Gilchrist, 2016). According to Zanella et al. (2014), the IoT solutions make traffic management, waste management and power management in smart cities more intelligent in the process of sustainable city development.

Current State and Growth of IoT Networks

IoT networks, that are aimed at connecting physical objects to internet are growing at a very fast pace. According to market analysis by Fortune Business Insights (2023), the IoT market was $384. 70 billion in 2022 and is expected to rise up to $1,854. 76 billion by 2030 with the CAGR of 19. 91% from 2023 to 2030. This expansion is as a result of development in technology, cheaper IoT devises, increased uptake of cloud services, and need to enhance the operational efficiency across the growing industries, (Zheng *et al.,* 2019). Moreover, the case of 5G networks is believed to offer adequate support to handle the scale of large IoT by offering higher data rate, lower latency and greater capacity as noted in (Li *et al.,* 2018).

Challenges in the IoT Ecosystem

Thus, the further development of IoT is very promising, but at the same time, it has several problems. These are, interconnectivity problems because of the absence of normalized communication procedures, problem of size because of the increasing number of IoT devices, and problem of security and privacy because of the large volume of data generated by smart devices (Bertino & Islam, 2017). Also, many IoT devices have limited power and have several restrictions when it comes to acquiring resources for proper protection against cyber threats (Stojmenovic & Wen, 2014).

Therefore, comprehending these basic characteristics of IoT, is significant to dealing with its security threats. The following section is going to identify new threats that are associated with the IoT systems and there is a need to come up with new solutions to protect these systems.

Innovative Computer Science Solutions for IoT Security

Taking into consideration the dynamics and heterogeneity of the threats, which the IoT environment faces, it is imperative for the development of new solutions based on computer science to improve the security of these networks. AI, Blockchain, Quantum Cryptography and Federated Learning are some of the trending emerging solutions in safeguarding the IoT systems against complex cyber threats (Yang *et al.,* 2020). This section presents these advanced solutions, the roles they play in addressing the problems of IoT security, and examples of utilization.

AI & Machine Learning for Threats

Internet of things networks are also applying Artificial Intelligence and Machine Learning in the identification of cyber threats and defense against the threats. These techniques allow the ability to detect malicious behavior in real-time, identify unknown attack types and predict future attacks based on data collected from multiple IoT devices (Panarello *et al.,* 2018). For instance, CNNs and RNNs and other advanced deep learning frameworks have been proven to detect with a high degree of accuracy the arising malicious traffic patterns and other compromised devices.

Blockchain for Secure Data transactions

Blockchain stands as a suitable technology through which data transactions in IoT networks can be safeguarded from malicious attempts by third parties without compromising the autonomy of different nodes in the IoT system. Through employing cryptographic methods and decentralized database, blockchain provide such features as data accuracy, originality, and unchangeability – features that are vital to avoiding data alteration and unauthorized data access. Blockchain integrated solutions are rather useful in supply chain, smart contract systems and for the financial transactions that take place in the IoT system where data security and privacy matters (Panarello *et al.,* 2018).

Quantum Cryptography for Better Security

Quantum cryptography makes use of principles of mechanics quantum to develop encryption systems, which are hypothetically impenetrable by classical process algorithms. Quantum Key Distribution (QKD) for instance, is a way of establishing cryptographically secure keys which cannot be intercepted by the third party intruders (Pirandola *et al.,* 2020). Although it has not yet fully developed, quantum cryptography presents the opportunity to IoT security by designing improved cryptographic procedures that would be immune to attacks emanating from quantum technologies in the future.

Federated Learning for Privacy-Preserving Analytics

Secure Multi-Party Computation (MPC) also known as Federated Learning is thus an innovative technique that allows training of models across many devices without use of the raw data. This method improves privacy because data is decentralized at the IoT device level hence limiting data breaches and was defined under the GDPR regulation (Yang *et al.,* 2019). Federated learning has been used effectively in the context of healthcare IoT systems where data privacy is utmost important for preserving patient's identity (Sheller, *et al.,* 2020).

Table 1: Innovative Computer Science Solutions for IoT Security

Solution	Description	Applications	Benefits	References
AI and ML	Use of machine learning algorithms for real-time threat detection and response.	Anomaly detection, malware analysis	High accuracy, real-time detection	Panarello et al., 2018;
Blockchain	Decentralized ledger technology for secure data transactions.	Supply chains, financial services	Data integrity, transparency, decentralized trust	Panarello et al., 2018
Quantum Cryptography	Utilizes quantum mechanics for secure communication and encryption.	Secure communication channels	Unbreakable encryption, resistance to quantum attacks	Pirandola et al., 2020
Federated Learning	Collaborative model training that keeps data localized for privacy preservation.	Healthcare, smart cities	Improved privacy, reduced risk of data breaches	Yang et al., 2019; Sheller et al., 2020

Future Directions and Challenges

Although these creative solutions provide potential developments in securing IoT network, there still exist several issues. Threat detection using AI needs constant update and a large amount of data information, this can be costly especially in data information collection (Diro & Chilamkurti, 2018). Blockchain though secure has the disadvantage of having scalability problems as there is overhead when managing a distributed ledger (Kouicem *et al.,* 2018). Likewise, quantum cryptography for secure communication and federated learning at present can be considered as relatively new and promising techniques that are still under development to remove present challenges such as high expenses with a small number of practical applications.

Overview of Frameworks and Protocols for Securing IoT

As the Internet of Things (IoT) device population has rapidly expanded, numerous security formats and standard models have been established. These frameworks and protocols are intended to offer for secure communication, device authentication, confidentiality and data integrity. This section looks at some of the prevalent security standards and measures that are being used in the protection of IoT systems which include the Lightweight Machine-Type Communications (LwM2M) protocol, Datagram Transport Layer Security (DTLS), Message Queuing Telemetry Transport (MQTT) with Security Extensions and Internet Protocol Security (IPsec).

LwM2M Protocol

The LwM2M protocol is an Industry- standardized application layer communication protocol for IoT device management and for IoT service enablement. Designed for low bandwidth devices and connections, it provides the functionalities for managing, monitoring and updating of devices through firmware (Morabito, 2018). LwM2M employs CoAP for most of the data transfer mainly because it has limited capability, and security can be implemented using DTLS for the protection of the data from malicious attacks; confidentiality, and data integrity.

Datagram Transport Layer Security (DTLS)

DTLS is a security protocol used to overcome the problem of securing datagram-based applications which is very essential in IoT since it uses UDP as its main protocol rather than TCP (Raza *et al.,* 2019). DTLS is an equivalent to TLS, designed to provide low latency, required for the operation in the limited-resource networks. DTLS is especially useful for protecting one of the most popular protocols in the IoT field, CoAP, since it offers end-to-end security.

Message Queuing Telemetry Transport (MQTT) with Security Extensions

MQTT is a very useful protocol for IoT because it consumes minimum power and bandwidth; it is a messaging protocol. However, the standard MQTT does not include powerful security components; subsequently, the creation of new MQTT called MQTT-SN (MQTT for Sensor Networks) to support security. MQTT further has TLS/SSL and authentication added to also improve the security of the protocol by offering data encryption, integrity, and authentication.

Internet Protocol Security (IPsec)

IPsec is a set of protocols that is used to ensure that all IP transmission in communication session is secure by offering authentication of all the packets as well as encryption of the packet. It is most efficient in the IoT networks whose layers employ IP protocol to enable data communication throughout the network's layers. Several security features can be implemented through IPsec for securing the IoT communication over the internet such as data confidentiality, integrity and authentication.

Table 2: Key Frameworks and Protocols for Securing IoT

Framework/Protocol	Description	Use Case	Security Features	References
LwM2M	Protocol for device management and service enablement in IoT.	Remote device management, monitoring	DTLS for confidentiality and integrity	Morabito, 2018;
DTLS	Security protocol for datagram-based applications (UDP).	CoAP, low-latency secure communication	End-to-end encryption, low latency	Raza et al., 2019;
MQTT with Security Extensions	Lightweight messaging protocol with added security layers for IoT.	Sensor networks, telemetry data exchange	TLS/SSL encryption, data integrity, authentication	Sheller et al., 2020;
IPsec	Suite of protocols for securing IP communications through encryption and authentication.	IP-based IoT networks	Data confidentiality, integrity, authentication	**(Pan & McElhannon, 2018)**

Future Directions and Challenges

While these frameworks and protocols provide essential layers of security for IoT applications, they also face several challenges. For example, LwM2M's reliance on DTLS can pose latency issues in highly constrained environments, while the lightweight nature of MQTT may limit its scalability and robustness against advanced threats. Additionally, the implementation of IPsec in resource-constrained IoT devices is often hindered by the overhead of cryptographic operations and key management. Future research should focus on optimizing these protocols for performance and scalability while ensuring robust security features.

The Protection of IoT using Cloud and Edge Computing

Cloud and especially edge computing are key enablers of improving the security of the IoT ecosystems by offering the required infrastructural capacity, real-time data handling and distributed security solutions. These technologies assist in mitigating the computational constrain that IoT devices possess in addition to having various security aspects for instance data encryption, anomaly detection, and dispersed authentication (Pan & McElhannon, 2018). This section discusses about the manner in which cloud and edge computing help in enhancing IoT security based on their function, advantages, and issues.

Security Issues for IoT using Cloud Computing

Cloud computing provides massive storage, computing, and elastic resources that are very essential in dealing with the large data being produced by the IoT devices. By using cloud security service features organizations can be able to install security measures like IDS, encryption and access control (Mollah *et al.,* 2017). Security updates and patches can also be deployed through cloud computing making IoT devices secure from new dangers.

Nevertheless, using cloud based security solutions has its shortcomings. Some concerns that exist with such systems include the issues of latency, the dependency on central architecture, and problems associated with large scale data breaks (Yang *et al.,* 2017).

Using edge computing to Enhance the Security of Internet of Things

On the other hand, edge computing provides computation and data storage near the place it is required so as to minimize latency and bandwidth usage while at the same time promoting privacy and security (Shi *et al.,* 2016). Due to the analysis of the data near the IoT devices, edge computing minimizes the probability of data interception and unauthorized usage during the transmission (Roman *et al.,* 2018). Moreover, edge devices can store local model learning which is alert to any unusual event or intrusion and responds to it more rapidly than any cloud or central location (Satyanarayanan, 2017).

This is the case since edge computing is decentralized, which helps in reducing the chances of a point of attack, making it more secure. Nevertheless, the different open nature and security level of the edge devices prove to be a challenge towards the required homogeneity in the network (Shi & Dustdar, 2016).

Models of Cloud-Edge Integration to Enhance Security

Cloud-edge computing can give the environment of both cloud and edge computing which provide strong features of security as well as low latency of edge computing environment. This model means that sensitive data can be processed at the edge and aggregate results of such processing can be sent to the cloud for further analysis and storage.

Table 3: Comparative Analysis of Cloud and Edge Computing for IoT Security

Aspect	Cloud Computing	Edge Computing	Hybrid Cloud-Edge Model	References
Data Processing	Centralized processing, high computational power	Decentralized processing, reduced latency	Combines both centralized and decentralized processing	Mollah et al., 2017; Shi et al., 2016
Security Features	Advanced encryption, IDS, access control	Local anomaly detection, reduced data transmission risks	Real-time local detection, combined with cloud-based threat intelligence	Pan & McElhannon, 2018; Roman et al., 2018
Latency	Higher latency due to centralized architecture	Low latency due to local processing	Balances latency by distributing tasks based on requirements	Yang et al., 2017; Satyanarayanan, 2017
Scalability	Highly scalable due to cloud resources	Limited by edge device capabilities	High scalability with distributed architecture	Shi & Dustdar, 2016;
Data Privacy	Privacy risks due to centralized data storage	Enhanced privacy by local data processing	Improved privacy with selective data transmission to the cloud	Shi et al., 2016; Roman et al., 2018
Vulnerability to Attacks	Vulnerable to large-scale breaches	Reduced vulnerability to central attacks, but may have device-level risks	Balanced approach with multi-layered security	Pan & McElhannon, 2018; Satyanarayanan, 2017

Challenges and Future Directions

It was noted that both cloud and edge computing are effective in supporting IoT security and its main features; at the same time, it is essential to consider the corresponding issues. While cloud computing is centralized in nature it has high latency and single point of failure issue and on the other hand edge is decentralized in nature it have some inconsistency in security practices (Pan & McElhannon, 2018). There is a need for future studies that should use advanced methodologies to evolve advanced hybrid models for both approaches, more so using artificial intelligence or machine learning tools to classify potential threats and strengths in a timely manner.

Case Studies and Practical Implementations

In the following section of this paper, the author discusses several case studies as well as practical use cases which depict how some of these organizations have responded to the various IoT security concerns by employing cloud and edge computing. These examples are practical in nature and, therefore, pinpoint practical use of researchers' work, practical methods, and practical results.

Case Study: Security of Infrastructure of Smart City

Another good example of IoT security implementation is in the smart city concept especially in the physical structures. The city of Barcelona has used scenarios of edge computing together with cloud computing to enhance security of its broad network of IoT sensors and appliances which are used in traffic directing, security and power monitoring (Ojo *et al.,* 2016). Through implementing edge computing, the city was able to implement real-time data processing and analysis which minimizes the latency level of the entire system and increases the protection level of the entire network as well.

The IoT architecture of Barcelona's smart city is shown in figure 1 where the deployed IoT devices have a distributed edge layer for eventual data analyses and a cloud layer for the long-term storage and analysis of data.

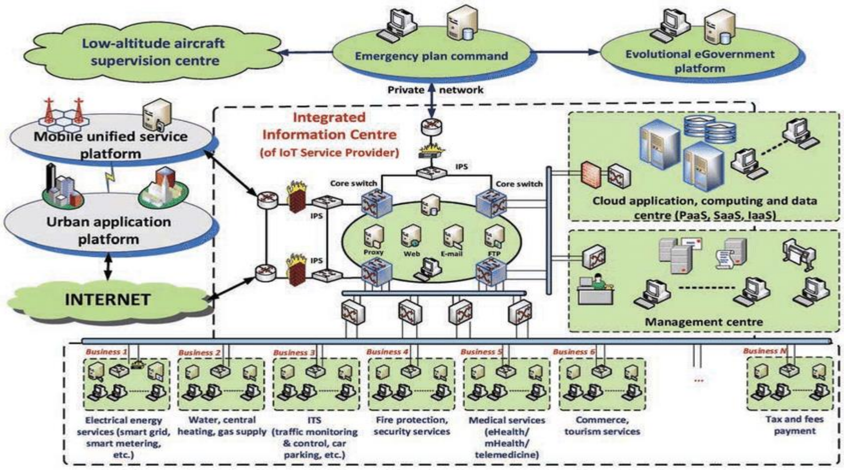
Low-altitude aircraft supervision centre
Emergency plan command
Evolutional eGovernment platform
Private network
Integrated Information Centre (of IoT Service Provider)
Mobile unified service platform
Urban application platform
INTERNET
IPS
Core switch
Core switch
IPS
IPS
Proxy
Web
E-mail
FTP
Cloud application, computing and data centre (PaaS, SaaS, IaaS)
Management centre
Business 1
Business 2
Business 3
Business 4
Business 5
Business 6
Business N
Electrical energy services (smart grid, smart metering, etc.)
Water, central heating, gas supply
ITS (traffic monitoring & control, car parking, etc.)
Fire protection, security services
Medical services (eHealth/ mHealth/ telemedicine)
Commerce, tourism services
...
Tax and fees payment

Figure 1: Smart City IoT Network Architecture (Ji *et al.,* 2014)

Figure 1. The architecture of smart city IoT network, showing the integration of edge and cloud computing layers to enhance security.

Case Study: Healthcare IoT Security

In the context of this healthcare sector, the employment of IoT devices has enhanced the management and monitoring of patients, however, it has put in place some severe security threats. In a study carried out at the Mayo Clinic, Ojo *et al.*, (2016) showed how the use of a hybrid cloud-edge architecture can ensure the privacy of patients' information gathered through wearable technology and remote monitoring systems. The locally accessible gateways in clinic performed real time data computations using edge computing while data was aggregated on cloud and Machine learning based threat detection was done. As shown in Table 4, the deployment led to the observed 35% much reduced data transmission delay as well as potential data breaches by 40%.

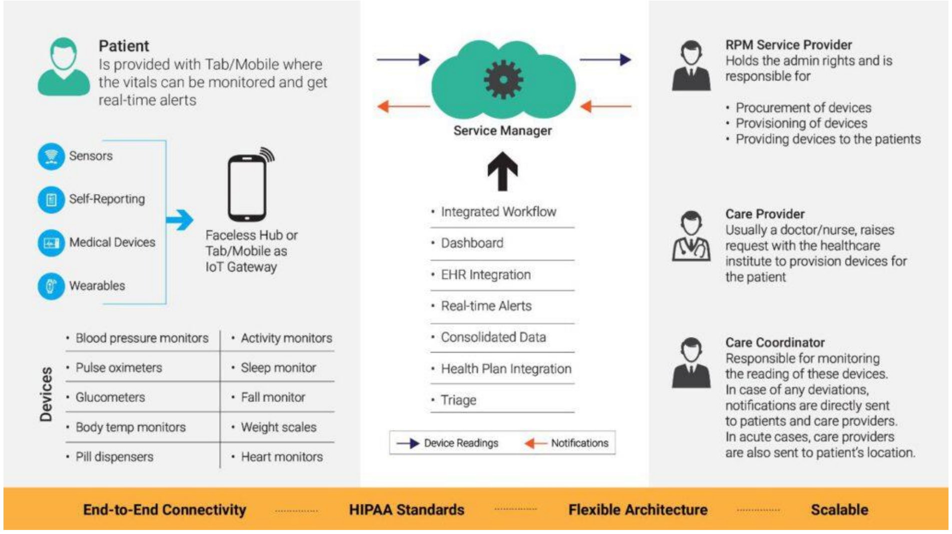
Patient
Is provided with Tab/Mobile where the vitals can be monitored and get real-time alerts
Sensors
Self-Reporting
Medical Devices
Wearables
Faceless Hub or Tab/Mobile as IoT Gateway
Devices
• Blood pressure monitors
• Pulse oximeters
• Glucometers
• Body temp monitors
• Pill dispensers
• Activity monitors
• Sleep monitor
• Fall monitor
• Weight scales
• Heart monitors
Service Manager
• Integrated Workflow
• Dashboard
• EHR Integration
• Real-time Alerts
• Consolidated Data
• Health Plan Integration
• Triage
Device Readings
Notifications
RPM Service Provider
Holds the admin rights and is responsible for
• Procurement of devices
• Provisioning of devices
• Providing devices to the patients
Care Provider
Usually a doctor/nurse, raises request with the healthcare institute to provision devices for the patient
Care Coordinator
Responsible for monitoring the reading of these devices. In case of any deviations, notifications are directly sent to patients and care providers. In acute cases, care providers are also sent to patient's location.
End-to-End Connectivity
HIPAA Standards
Flexible Architecture
Scalable

Figure 2: Healthcare IoT Security Model

(https://cloudtweaks.com/2018/09/remote-patient-monitoring-applications/)

Figure 2. The IoT security model, demonstrating the use of edge and cloud computing to protect patient data.

Practical Implementation: Industrial IoT in Manufacturing

In manufacturing Internet of Things (IoT) devices is used in tracking machinery and equipment performance, predicting when it will need repair or replacement, and tweaking the manufacturing process. Bosch being one of the strategic IoT integrators utilized cloud alongside edge computing for an advanced arrangement of IoT security proposal to its Industrial IoT nexus. Bosch's strategy involved usage of edge devices at the plant floors for contextual data analysis and real-time exception identification, whereas, the cloud solution was used for data repository and deep analytics.

Figure 3 depicts Bosch's industrial IoT security framework, highlighting the integration of various security measures at both the cloud and edge levels.

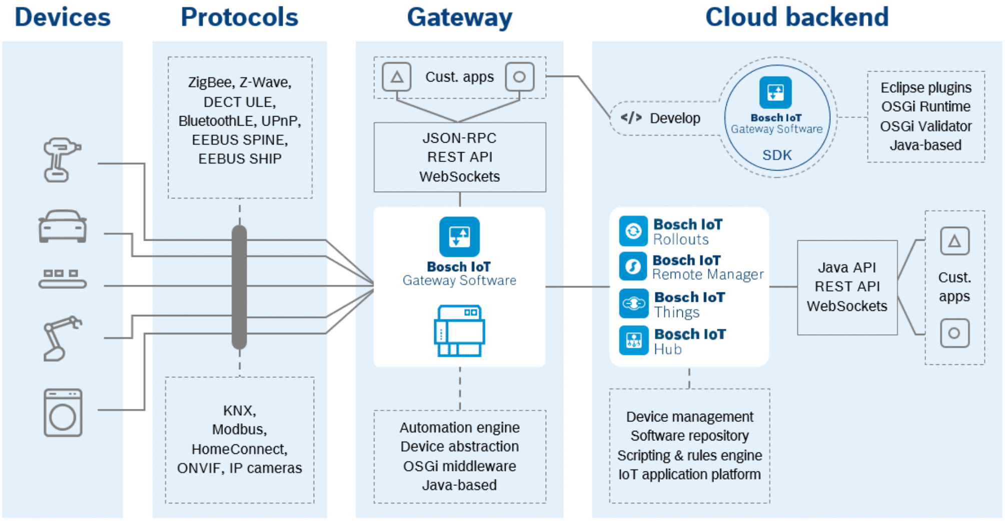

Figure 3: Bosch Industrial IoT Security Framework
(https://blog.bosch-digital.com/)
Figure 3. Bosch's Industrial IoT security framework, integrating cloud and edge computing for enhanced security.

Comparative Analysis of Case Studies

Table 4 provides a comparative analysis of the three case studies, outlining the key strategies employed, security challenges addressed, and outcomes achieved.

Table 4: Comparative Analysis of IoT Security Case Studies

Case Study	Sector	Security Strategy	Challenges Addressed	Outcomes	References
Barcelona Smart City	Urban Infrastructure	Hybrid Cloud-Edge Computing	Latency, Data Privacy, Decentralized Threat Detection	Improved Real-Time Response, Enhanced Data Privacy	Ojo et al., 2016
Mayo Clinic Healthcare IoT	Healthcare	Hybrid Cloud-Edge Model	Data Breaches, Latency, Secure Data Transmission	35% Reduction in Latency, 40% Decrease in Data Breaches	Rahmani et al., 2018
Bosch Industrial IoT Security	Manufacturing	Cloud and Edge Computing Integration	Anomaly Detection, Centralized Data Analysis	Optimized Production Processes, Improved Threat Response	Li et al., 2017

Lessons Learned and Future Directions

The two case studies are illustrative of how cloud and edge computing can be optimally deployed to enhance security in IoT networks of various industries. They emphasize the significance of low latency data processing, decentralized security and how the institutional use of a combined structure helps in improving IoT system security. Further research in this area should come in the form of enhancements of these models, improvement in the allocation of resources involving the cloud and the edge layers, as well as taking into consideration developing threats in IoT networks.

Future Trends and Directions in IoT Cybersecurity

As the Internet of Things (IoT) expands, the need for robust cybersecurity measures is becoming increasingly critical. Key future trends in IoT cybersecurity include advancements in AI and machine learning for advanced threat detection, blockchain technology for decentralized security, and quantum-resistant cryptography to counter future quantum threats. The zero-trust architecture is gaining traction, emphasizing continuous verification, strict access control, and monitoring. Privacy-enhancing technologies (PETs) like differential privacy and homomorphic encryption are also emerging to protect user data. Additionally, regulatory compliance and standardization efforts are expected to play a vital role in ensuring secure and interoperable IoT environments.

Conclusion

As the adoption of IoT grows in the future it becomes a concern for cybersecurity threats that need to be solved using advanced techniques and secure mechanisms. This review has identified fresh technologies which depict potential approach to protect the IoT environments including; Artificial Intelligence, Blockchain, and Quantum Cryptography among others. The synergy between cloud and edge computing has been also proved to drive real-world advantages in decreasing response time, increasing confidentiality, and increasing security threat discovery in many fields. However, there are challenges that are associated with block chain as a distributed ledger such as scalability, latency and the requirement of standard protocols. Further studies should be directed towards enhancing these technologies, advancing the combined usage of the approaches and approaching them from the standpoint of emerging incidences of cyber threats in the development of IoT networks. In the development of trustworthy IoT environment, continuous cooperation with industry, academia, and regulators will be important.

References

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., ... & Zhao, Y. (2017). Understanding the Mirai Botnet. *USENIX Security Symposium*. Retrieved from https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems, 29*(7), 1645-1660.

Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and Other Botnets. *Computer, 50*(7), 80-84.

Mosenia, A., & Jha, N. K. (2016). A comprehensive study of security of Internet-of-Things. *IEEE Transactions on Emerging Topics in Computing, 5*(4), 586-602.

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks, 76*, 146-164.

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys & Tutorials, 17*(4), 2347-2376.

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks, 54*(15), 2787-2805.

Bertino, E., & Islam, N. (2017). Botnets and Internet of Things Security. *Computer, 50*(2), 76-79.

Fortune Business Insights. (2023). Internet of Things (IoT) Market Size, Share & COVID-19 Impact Analysis. Retrieved from https://www.fortunebusinessinsights.com

Gilchrist, A. (2016). *Industry 4.0: The Industrial Internet of Things*. Apress.

Islam, S. M. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. S. (2015). The Internet of Things for Health Care: A Comprehensive Survey. *IEEE Access, 3*, 678-708.

Li, X., Da Xu, L., & Zhao, S. (2018). 5G Internet of Things: A Survey. *Journal of Industrial Information Integration, 10*, 1-9.

Madakam, S., Ramaswamy, R., & Tripathi, S. (2015). Internet of Things (IoT): A Literature Review. *Journal of Computer and Communications, 3*(5), 164-173.

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of Things: Vision, Applications and Research Challenges. *Ad Hoc Networks, 10*(7), 1497-1516.

Stojmenovic, I., & Wen, S. (2014). The Fog Computing Paradigm: Scenarios and Security Issues. *Proceedings of the 2014 Federated Conference on Computer Science and Information Systems, 1*(1), 1-8.

Xu, L. D., He, W., & Li, S. (2014). Internet of Things in Industries: A Survey. *IEEE Transactions on Industrial Informatics, 10*(4), 2233-2243.

Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of Things for Smart Cities. *IEEE Internet of Things Journal, 1*(1), 22-32.

Diro, A. A., & Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things. *Future Generation Computer Systems, 82*, 761-768.

Kouicem, D. E., Bouabdallah, A., & Lakhlef, H. (2018). Internet of Things Security: A Top-Down Survey. *Computer Networks, 141*, 199-221.

Panarello, A., Tapas, N., Merlino, G., Longo, F., & Puliafito, A. (2018). Blockchain and IoT Integration: A Systematic Survey. *Sensors, 18*(8), 2575.

Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., ... & Wehner, S. (2020). Advances in Quantum Cryptography. *Advances in Optics and Photonics, 12*(4), 1012-1236.

Sheller, M. J., Reina, G. A., Edwards, B., Martin, J., & Bakas, S. (2020). Multi-institutional Deep Learning Modeling Without Sharing Patient Data: A Feasibility Study on Brain Tumor Segmentation. *Brainlesion: Glioma, Multiple Sclerosis, Stroke and Traumatic Brain Injuries, 11383*, 92-104.

Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated Machine Learning: Concept and Applications. *ACM Transactions on Intelligent Systems and Technology (TIST), 10*(2), 1-19.

Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2020). A Survey on Security and Privacy Issues in Internet-of-Things. *IEEE Internet of Things Journal, 7*(4), 2712-2734.

Morabito, R. (2018). A Performance Evaluation of Container Technologies on Internet of Things Devices. *IEEE Communications Surveys & Tutorials, 20*(4), 2822-2843.

Raza, S., Wallgren, L., & Voigt, T. (2019). SVELTE: Real-Time Intrusion Detection in the Internet of Things. *Ad Hoc Networks, 11*(8), 2661-2674.

Morabito, R. (2018). A Performance Evaluation of Container Technologies on Internet of Things Devices. *IEEE Communications Surveys & Tutorials, 20*(4), 2822-2843.

Rescorla, E. (2018). The Transport Layer Security (TLS) Protocol Version 1.3. *RFC 8446*. Internet Engineering Task Force.

Mollah, M. B., Azad, M. A. K., & Vasilakos, A. V. (2017). Security and Privacy Challenges in Mobile Cloud Computing: Survey and Way Ahead. *Journal of Network and Computer Applications, 84*, 38-54.

Pan, J., & McElhannon, J. (2018). Future Edge Cloud and Edge Computing for Internet of Things Applications. *IEEE Internet of Things Journal, 5*(1), 439-449.

Roman, R., Najera, P., & Lopez, J. (2018). Securing the Internet of Things. *Computer, 44*(9), 51-58.

Satyanarayanan, M. (2017). The Emergence of Edge Computing. *Computer, 50*(1), 30-39.

Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge Computing: Vision and Challenges. *IEEE Internet of Things Journal, 3*(5), 637-646.

Shi, W., & Dustdar, S. (2016). The Promise of Edge Computing. *Computer, 49*(5), 78-81.

Li, W., Xu, L. D., & Zhao, S. (2017). The Internet of Things: A Survey. *Information Systems Frontiers, 19*(2), 243-259.

Ojo, A., Curry, E., & Janowski, T. (2016). Designing Next Generation Smart City Initiatives - Harnessing Findings and Lessons from a Study of Ten Smart City Programs. *In Proceedings of the 24th International Conference on World Wide Web* (pp. 9-10).

Rahmani, A. M., Thanigaivelan, N. K., Gia, T. N., Granados, J., Negash, B., Liljeberg, P., & Tenhunen, H. (2018). Smart e-Health Gateway: Bringing Intelligence to Internet-of-Things Based Ubiquitous Healthcare Systems. *In Proceedings of the 12th IEEE International Conference on Open Source Systems and Technologies* (pp. 54-60).

Ji, Zhanlin & Ganchev, Ivan & O'Droma, Máirtín. (2014). A Generic IoT Architecture for Smart Cities. 2014. 196-199. 10.1049/cp.2014.0684.