International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 12, No.1 (Oct-2022)

https://dx.doi.org/10.12785/ijcds/120198

Challenges for Security in IoT, Emerging Solutions, and Research Directions

Iraq Ahmad Reshi[1] **and Sahil Sholla**[1]

[1]*Department of Computer Science and Engineering, Islamic University of Science and Technology, Kashmir, JK, India*
Received 22 Jan. 2021, Revised 15 Jul. 2022, Accepted 23 Jul. 2022, Published 1 Oct. 2022

Abstract: : Internet of Things (IoT) systems have gained huge popularity in the past decade. This technology is developing as a back boon from the day-to-day utility in smart homes to intelligent power grids. It has become ubiquitous in the past decade while gaining popularity in academia and industry. As the devices used are usually sensors without a well-developed user interface, they are vulnerable to various threats. In this survey article, we have undergone some of the security challenges the technology faces and how the recently emerging technologies can provide an escape. Emerging technologies like blockchain, AI, and Deep learning techniques provide a platform where IoT operations are carried out successfully and securely. However, specific challenges need to be dealt with before implementing these in practice. We have briefly reviewed the role of particular technologies in securing IoT devices.

Keywords: Fog Computing, Blockchain, Quantum Cryptography, Tiny Encryption, Machine Learning, Deep Learning

1. Introduction

By 2025, the total deployment of Internet of Things (IoT) linked devices is predicted to reach 30.9 billion elements, a significant increase from the 13.8 billion devices that were expected by the end of 2021[1]. IoT architecture include Sensing layer, which is the data collection layer, the Network layer which undertakes the communication part, and the application layer that enables services and user interface. A typical IoT architecture where data collected from sensors is transmitted to the cloud via a gateway as shown in figure 1. The data can be visualized at a user interface. The four-layer architecture includes separation of application and services and the five-layer architecture further adds a business layer over the application layer. Though IoT has found a vast application in several areas including Healthcare, Vehicular traffic management, smart homes, smart cities, and a lot more, still it poses certain challenges that need to be addressed. Since an IoT network is mainly composed of sensors with limited device capabilities like battery and processing so there is a lot of management and operational issues other than traditional networks. A lot of IoT features have included vulnerabilities. With the heterogeneous nature of devices and by their interconnection a lot of interfaces need to be integrated. Hence it becomes more difficult to secure the system using one security protocol[2].

As IoT is the fusion of sensor networks with traditional network systems, it brings extra security vulnerabilities with its existence. Some researchers call it the Internet of Threats due to its weak secure infrastructure [3]. With the number of connected devices still on the rise, users feel insecure about the privacy and security issues, due to the heterogeneity of protocols and devices. In the past decade, several important surveys have been written on the topic. Tables 1 and 2 discuss the contribution of multiple researchers. Moreover, table 2 summarizes the contribution of proposed research articles considering the technological solutions discussed. The primary focus of our survey is to introduce the subjects to the broader scope of cutting-edge technologies that are enormously promising security solutions for IoT systems. These technologies will revolutionize the context of IoT networks in the near future. The rest of the paper is organized as follows. Section 2 briefs about various IoT security challenges. Section 3 describes the emerging technology solutions including Machine Learning (ML), Blockchain, Tiny encryption, Quantum resistant approaches, and Fog and edge computing. Section 4 briefs about the future research motivation. In section 5, we conclude the survey.

2. Security Challenges

The lack of a proper interface in IoT devices adds to their vulnerability. In past years we witnessed various large-scale IoT attacks that changed the whole perspective of security. Mirai malware generated data in terabytes by using common factory default User-id and passwords. It took down thousands of systems in 2016 and is still active [15]. Similarly, Stuxnet targets programmable logic controllers (PLCs), initially destroyed plants in Iran, and is active still and not domain-specific [16]. According to a CNN report in 2017, implantable medical devices possess vulnerabilities

E-mail address: rshiraq333@gmail.com, sahilsholla@gmail.com

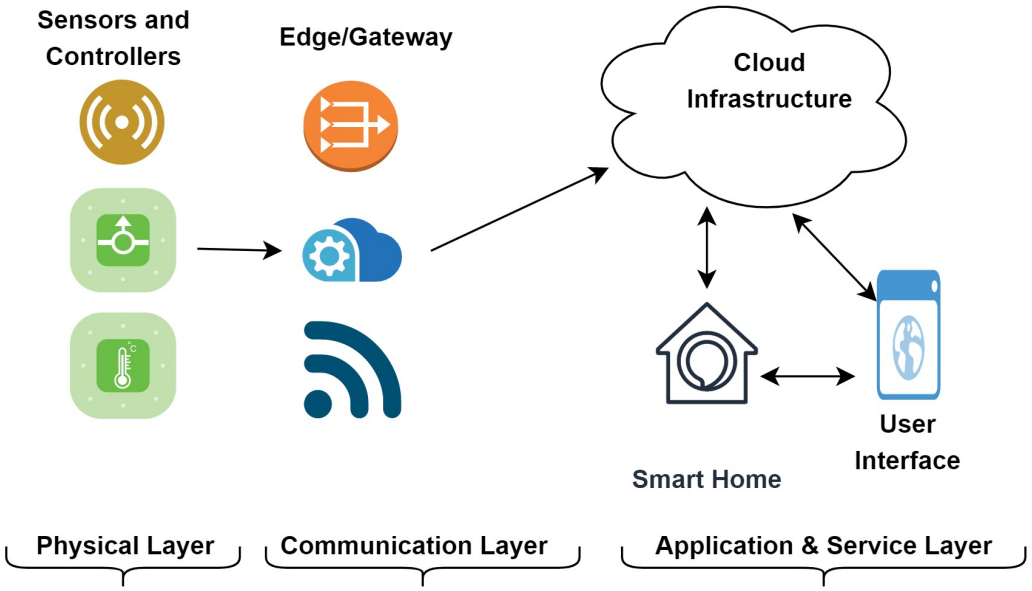

Figure 1. General architecture of an IoT network

that can be exploited. Such exploits can cost lives as the implantable devices include pacemakers and defibrillators that run the lives of hundreds of patients [17].In 2021 researchers discovered malware-based in an open-source programming language of google called BotenaGo [18].It has the ability to infect thousands of gateways and IoT devices. BotenaGo was identified by ATT AlienLabs engineers and can target over 30 distinct vulnerabilities.

IBM security intelligence reported a few years ago, a jeep was hacked and it was discovered that hackers could make it speed up or down that could cost human lives [19]. The various security concerns that need to be taken care of in an IoT system are mentioned below.

A. *Scalability*

The scalability issue arises due to the number of IoT devices constantly increasing. Making such a massive number of devices communicate is a big challenge. To connect considerable number of devices, traditional routing protocols are not suitable. Also, there is a need for data processing and management systems that can handle such significant data amounts. Due to a large number of nodes in IoT networks, a security mechanism designed for such a system should be scalable.

B. *Centralization*

As IoT devices cannot themselves handle the data and the related processing, a need for centralized architecture to process the data for the application layer is mandatory. The communication in an IoT network is so intense that these centralized systems may crash and render the network useless. A central server is also the target for most of the attacks. Centralized systems are prone to central system attacks from Citi-bank 1995 to Wana-cry 2017, and attackers plundered billions of dollars by targeting the vulnerabilities in centralized systems. IoT networks, due to the absence of sophisticated hardware at the end-user level, are more reliant on centralized servers for processing and communication. This factor increases the probability of Dos and DDoS attacks on IoT networks. Security solutions need to be devised such that the reliance on a central server is minimized and the probability of such attacks is minimized.

C. *Data Privacy*

Technological advancements in IoT have made us quite dependable on smart devices. The large-scale use of smart bands, Fitbit sensors, smart toys, and a lot more has complicated online data storage in terms of its privacy feature. The private data gets shared with unknown parties, and it may prove fatal in certain cases. Privacy feature has an immense requirement in IoT systems, especially when dealing with sensitive data like medical or smart homes. Radio Frequency utilization (RFID) and other tagging approaches used in IoT networks can largely reveal confidential information about the individual. The occurrence of eavesdropping and traffic analysis attacks in IoT networks is common due to their wireless nature, so approaches are

TABLE I. Key contribution of surveys published from 2014 to 2022

Reference	Year	Contribution
[4]	2014	Survey highlights the information security background in IoT systems, and various security challenges.
[5]	2015	A review of 100 symmetric ciphers including modern block, involution and lightweight ciphers utilized in resource constrained environments.
[6]	2016	Survey on challenges faced in common IoT implementations with solutions applicable at layer level.
[7]	2017	Taxonomy of current IoT security vulnerabilities in context of application, architecture and communication.
[8]	2018	Research trends in IoT from 2016 to 2018, with modellers, simulators and computational and analysis platforms.
[9]	2018	Survey on role of blockchain based mechanisms in securing IoT systems.
[10]	2019	Security related challenges in IoT and survey of technologies focussing on higher levels of integrity in IoT applications.
[11]	2020	A survey on State of art deep learning and big data technologies based solutions for plugging IoT vulnerabilities.
[12]]	2021	Discussion on Post Quantum cryptographic solutions for IoT systems with special mention of Lattice based cryptography.
[13]	2022	Complete quality analysis on authentication and session keys, in IoT systems and utilization of ML and blockchain in IoT systems for security purposes.
[14]	2022	A survey on symmetric and asymmetric light weight encryption algorithms for IoT systems.
This Survey	2022	A survey on cutting edge emerging technology security solutions for IoT systems.

required to tackle the different attacks leading to privacy breaches.

D. Protocol Interoperability

One more factor that adds to the constraints is the nature of IoT devices. Since they are heterogeneous, it implies a requirement of an infrastructure that takes into consideration the various types of devices and different natures. Also, an efficient routing scheme is needed to carry out the communication from the physical to the application layer. The interoperability feature of IoT networks should not hinder the security parameters, and similarly, the security mechanism applied should not limit the interoperability of the systems.

E. Data management

In IoT systems, data from multiple sources is collected and is subjected to multiple operations like prediction and mining. Due to the extremely large number of IoT devices, a huge amount of data is generated, and managing such a huge amount of data that is unstructured is a cumbersome task. Data management challenges in IoT systems include integrating the data taken from different sources, automation and distribution of the data collection process, and real-time analysis of the collected data. Mismanagement of IoT data gives rise to various security issues like confidentiality breaches. The confidential data in IoT networks needs to be protected using cryptographic primitives.

3. Promising Solution Approaches

Promising countermeasures for IoT security issues have been included in this paper.

A. Edge and Fog Computing

The cloud, IoT end devices, the edge, and users are all significant players in the edge-centric IoT architecture. Technology adopters employ sophisticated IoT apps to make their jobs easier, and instead of directly engaging with IoT end devices, they connect with them through the cloud or edge-based interactive interfaces [20].
Because of the inherent limitations of IoT technology, such as insufficient storage and processing capacity, a strong foundation is required to handle data efficiently. Fog computing is a technique that was proposed for bridging the gap between remote data centers and Internet of Things devices. Fog is an ideal framework for IoT services in a variety of applications, including linked cars and smart grids [21]. In [20] authors proposed EdgeSec, a concept for an innovative security service that is incorporated at the edge layer to improve IoT system security. EdgeSec is made up of several primary components that collaborate to address particular security concerns in IoT infrastructure methodically with effectiveness illustrated in the Smart home scenario. SIOTOME [22], another cooperative framework in between the access point and the Internet Service Provider (ISP) to provide real-time cyber security for detecting and isolating IoT security breaches. It is an architecture for a cohesive, privacy-preserving analytics architecture between the network edge and an ISP. Researchers developed a new programmable security architecture based on edge computing that uses a security agent as an approaching edge device to provide security services as IoT resources for the security requirements of all protocol stacks, including different applications [23].

TABLE II. Solution approaches analyzed in previous surveys for security in IoT

Reference	Title	Fog/Edge	Blockchain	ML/DL	Quantum Cryptography	Tiny Encryption
[4]	IoT Security: Ongoing Challenges and Research Opportunities.	-	-	-	-	✓
[5]	A comprehensive survey of modern symmetric cryptographic solutions for resource constrained. environments	-	-	-	-	✓
[6]	A Review of Security Concerns in Internet of Things.	-	-	-	-	-
[7]	Internet of Things security: A survey.	✓	-	-	-	✓
[8]	Current research on Internet of Things (IoT) security: A survey.	-	✓	-	-	✓
[9]	Blockchain mechanisms for IoT security.	-	✓	-	-	-
[10]	A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures.	✓	✓	✓	-	-
[11]	Deep learning and big data technologies for IoT security.	-	-	✓	-	-
[12]	Post-Quantum Cryptosystems for Internet-of-Things: A Survey on Lattice-Based Algorithms.	-	-	-	✓	-
[13]	Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence based key-security.	-	✓	✓	-	-
[14]	Lightweight cryptography in IoT networks: A survey.	-	-	-	-	✓
This Survey	Emerging Security Challenges and Promising Solution Approaches in IoT.	✓	✓	✓	✓	✓

This framework is intended to address issues such as high computing costs, limited key management versatility, and incompatibility when implementing new security algorithms in IoT, particularly when using complex encryption algorithms. A new framework to tackle the security of edge computing by virtualizing the edge nodes, which reduces the risks associated with data transfer[24]. Combining edge computing with virtual networks, as well as using network virtualization technologies to address the issues that edge are the future research areas in this topic. When dealing with highly sensitive data, such as in business or research, IoT devices are vulnerable to a variety of risks, which might result in data loss. Additional security can be obtained by performing additional computations on encrypted files as proposed in [25]. Homomorphic encryption is an encryption approach that permits calculations on encrypted data without decryption, avoiding the need to reveal the plaintext to intermediaries (servers). In [26], authors propose an Elliptic Curve Diffie–Hellman Ephemeral (ECDHE) with Pre-Shared Key (PSK). This integration was proposed as a lightweight authentication scheme based on the MQTT protocol. The suggested ECDHE-PSK technique is about as lightweight as the PSK method while having security features of certificate-based algorithms, according to the rigorous performance and security assessments. A service is created in which data and inferences from the edge are integrated with cloud insights to create a coherent system for early detection of security concerns and autonomous action, as well as alerting the user and ISP.

B. Blockchain

A blockchain is a distributed ledger that records all completed transactions and data in chronological sequence in a collection of tamper-proof memory space. These transactions are then shared among all individuals that have signed up. Every user or node in the system preserves the

very same ledger as other users or nodes in the network, information is kept and/or publicized as a shared ledger that is hard to alter [9]. The stability of the network is maintained by a mechanism called consensus, where nodes agree on certain conditions. There are several consensus mechanisms, different blockchain networks follow. In this regard, to converge IoT and blockchain technologies and how the latter comes as a savior for the former a deep study of the topic is intended. Blockchain-based IoT infrastructure is diagrammatically represented in figure 2. A survey on integration of blockchain with IoT, as well as the weaknesses of centralised designs like IoT and how role of blockchain in mitigating them is presented in [27]. Blockchain technologies when collaborated with IoT have a lot of technical issues like scalability, privacy, and various integration interfacing issues. Authors in [28] proposed sliding window blockchain architecture, for IoT as only a portion of the chain, is maintained in the device's memory instead of full node strength (n). By this, the memory constraints of IoT devices and scalability issues of blockchain are nullified. Litichain architecture is proposed based on End of graph (EOG) structure-based ordering of end time of blocks [29]. A block is removed from the chain after its lifetime expires, so in this way, it solves the memory constraint of IoT devices too. In [30], authors suggested a mechanism to control access to vital sensor and actuator data, via a private and lightweight blockchain. Real-time encryption techniques are performed on a minimal ARM Cortex-M4 microcontroller, and a massively scalable and energy-efficient consensus mechanism proof of authentication (POAH) is implemented on blockchain to improve the proposed architecture's computing performance. In [31] , authors provide a detailed summary of how to adapt blockchain to specific IoT requirements to create blockchain-based IoT (BIoT) applications, intending current state-of-the-art effort in this area. Despite the limitations and open security vulnerabilities that blockchain may impose on present IoT systems, In [32], authors explored IoT security and privacy issues and how blockchain might be used to solve these issues. Moreover, this paper summarizes the results of blockchain and IoT upon integration with machine learning as the integration promises enhanced security mechanisms. Moreover, researchers outlined the fundamental issues that IoT systems face, as well as blockchain's potential role in addressing them. The novelty of introducing dew and cloudlet technologies enhances the throughput by reducing end-to-end delay as the computing is done closer to IoT devices in this approach[33].

C. Machine And Deep Learning

Implementing security protocols for IoT devices such as encryption, authentication, identity management, network, and information protection, is inefficient[4]. As a result, existing security approaches need to be improved to safeguard the IoT ecosystem properly. Machine learning and deep learning (ML/DL) have come a long way in recent years, and machine intelligence has gone from being a laboratory curiosity to being used in a variety of essential applications [34]. Figure 3 represents the integration of ML or DL approaches with IoT infrastructure. The deep and Machine Learning-based approach has a great advantage over traditional security systems while tackling Zero-day attacks. As the algorithms based on Deep Learning are powerful analyzing tools for learning normal or abnormal behavior. Collecting input data from the IoT devices and analyzing the communicating pattern, enable us to identify malicious behavior at an early stage [35]. The authors in [36] introduced a new machine learning (ML)-based security architecture that can automatically deal with the growing security concerns in the IoT area utilizing the data mining methods. This reviewed experiment for the anomaly-based intrusion detection system (IDS) for IoT in a real Smart building scenario is proven to be extremely successful. In [37] authors described a wireless device recognition platform that uses deep learning approaches to improve Internet of things (IoT) security.

Deep learning is a potential way for learning the properties of various radio frequency (RF) devices based on their RF data. To recognize digital devices and differentiate among devices from the same manufacturer, three deep learning models considered are Deep Neural Network (DNN), Convolutional Neural Network (CNN), and Recurrent Neural Network (RNN). As a physical layer authentication system, RF fingerprinting might be used to differentiate genuine wireless devices from malicious ones. Moreover, Deep Learning methods can predict unknown attacks that are mutants of the known or previous ones. As they learn and train from the previous examples and predict the future [34] . Researchers in [38] proposed an IDS which employs ML to detect cyber-attacks and inhomogeneities in IoT networks with limited resources. CICIDS2017 and NSL-KDD datasets were subjected to extensive testing and training and the results showed the model can spot malicious activity with considerably fewer training examples and training time. Another such approach was proposed in [39] that proposes a Deep Learning-based anomaly detection system for IoT networks. This model is also safe from illegal authentication and malicious activities. Recently advancements in Federated Learning also show a lot of promise in countering IoT security issues, especially privacy. In this mode of learning, the modules can be trained and the learning process can be distributed across the different nodes. A study in[40] proposes a federated learning method that combines an adaptable gradient descent approach with a differential privacy technique for multi-party participatory modeling contexts. Under fixed communication costs, the suggested dynamic federated learning approach outperforms standard methods, according to experimental results.

D. Quantum Cryptography

Due to the inevitable advent of scalable quantum systems, substantial research in Post Quantum Cryptography (PQC) has sprung up. Embedded IoT (edge) devices have a greater difficulty due to their widespread use in today's

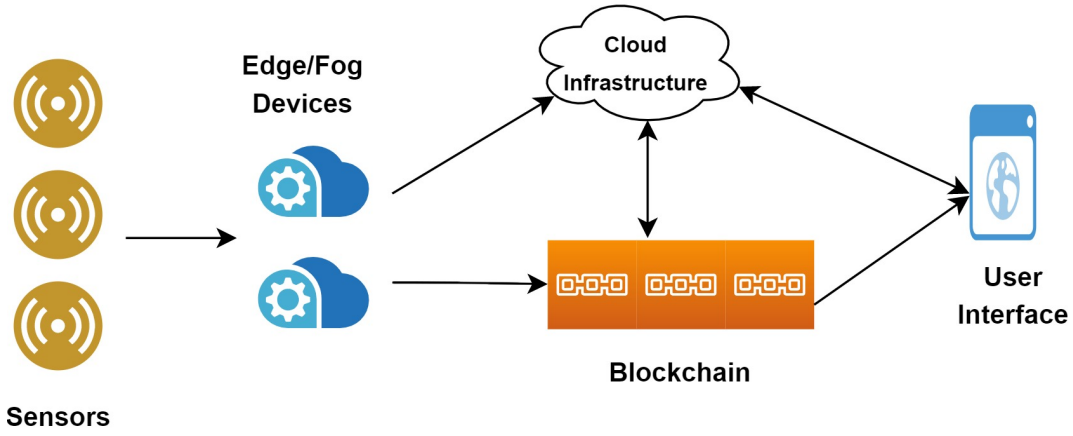

Figure 2. Blockchain-based IoT system

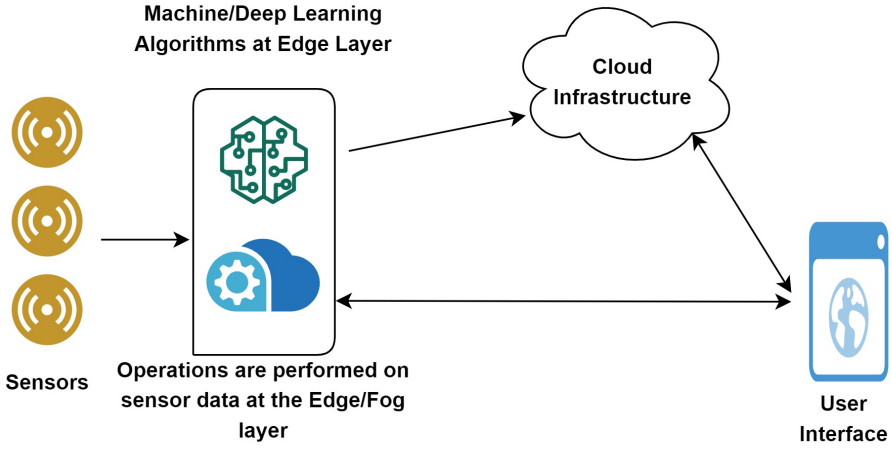

Figure 3. Machine and Deep Learning integration with IoT system

society and their more stringent resource. Lattice-based Encryption (LBE) is emerging as one of the most feasible quantum-resistant cryptography schemes about half of the survivors of the second round of the NIST's PQC challenge are lattice-based in structure [41].

In [42], a hybrid IoT security framework with an additional layer that assures quantum state is proposed. By preserving its state and securing the key with quantum cryptography BB84 protocol, this state prohibits eavesdroppers from doing damaging operations in the transmission medium and cyberspace. The hybrid management employs a traditional cryptographic mechanism known as One-Time Pad (OTP). The article [43] provides an overview of what is known as post-quantum IoT systems (IoT systems that are immune to presently available quantum attacks. Post quantum security with special reference to IoT systems is discussed. In [44] researchers proposed IoT combining quantum key distribution (QKD) and the RC6 encryption algorithm, where QKD is the scientific method of exploiting the subatomic particles effect to execute security tasks and produce a secret key. QKD is a quantum key distribution system that uses photons to produce a key and sends data across a quantum channel, also known as a fiber optic channel or optical free space. Utilized BB84 protocol by Bennett and Brassard (1984). The BB84 methodology creates a keystream between two people based on the polarization of the photon to capture the state of the particle, which is known as a qubit (in quantum theory, a qubit can be both 0 and 1 at the very same time) and then converts it to a regular bit predicated on the photon polarization. In another approach proposed in [45]

called new bilateral generalization inhomogeneous short integer solution (Bi-GISIS). This solution is implemented with the re-useable key feature. Because recyclable keys are ensured, a similar key can be used in multiple iterations of the suggested technique. This capability lets resource-constrained IoT designs make efficient use of reusable keys. PQ-FLAT [46] is a lightweight cryptographic protocol for enhancing the security of IoT devices. It is based on the unified lightweight identification of artifacts,that performs well in IoT networks for resource-constrained gadgets. A lattice-based encrypted communication technique is employed rather than the asymmetrical cryptosystem, which is reliable throughout the post-quantum world.

E. Tiny Encryption

Due to sluggish nature of traditional cryptographic methods, lightweight cryptography centered on Tiny Encryption Algorithms (TEA) is required to improve performance benefits from a software perspective instead of hardware implementation for IoT devices. These techniques shorten the time it takes to encrypt data in the IoT platform while maintaining the security-efficiency trade-off[47]. The algorithms for an IoT-driven setup should be more safe and efficient, as well as more suited to data security [19]. But TEA suffers from several issues like equivalent and related key attacks [48].
Lowering the encryption round in PRESENT cipher resulted in a lightweight PRESENT cipher by changing the Key Register updating mechanism, and adding an extra layer between the S-box layer and the P-layer of the existing cryptographic method. The additional layer allows us to lower the PRESENT round from 31 to 25, which is the bare minimum necessary for security. Encrypting the key register improves the performance of the proposed technique [49]. Authors in [50] sought to improve the security of smart home devices by creating a new TEA. Through entropy shifting, expanding, and mixing techniques, TEA's weaknesses of related-key attacks and the vulnerability of predictable keys were removed, allowing it to be used in protecting smart devices. With the same keys, the updated TEA generates different ciphertext. The modified TEA was shown to be more secure than the original TEA in testing. Another study provides a Dynamic Light-weight Symmetric (DLS) encryption method that was conceived and built to handle data security and real-time reliable data transfer via message advertising [51]. The algorithm encrypts each sending packet using a basic XOR operator using a unique periodic encryption method. DLS can dramatically improve security over existing baseline cryptographic algorithms with only a minimal increase in computer requirements. Recently Nayak et al., [52] proposed a lightweight algorithm for encrypting IoT data called Enhanced Secure IoT (ESIT). It is a block cipher-based approach that utilizes a 64-bit key. By deleting the string of q-bits from each lateral side, it is the typical bitwise left and right shift. The experimental analysis clearly shows the advantages of the proposed approach. In [53] Islam et al., the authors proposed an approach that ensures a smooth lightweight security approach that relies on Elliptic Curve Cryptography is described to secure interaction between IoT devices. It defends typical malware and offers total protection against security concerns such as identification, privacy, stability, and key exchange. Experimental evaluation shows that the suggested method outperforms state-of-the-art cryptographic algorithms.

F. Other Techniques

Apart from mentioned emerging technologies, there are other approaches that can be utilized for securing IoT infrastructures. Software defined networking (SDN) is one such platform that introduces SDN controller that manages the whole network. SDN, from a security standpoint, does have capacity to collect data from connected devices and enable programs to control forwarding devices, unleashing a powerful tool for adaptive and intelligent security policies [54]. The key focus of researchers for secure IoT architectures have been towards software based solutions, however, hardware based solutions have started to gain popularity in recent times. In [55], a physical unclonable function (PUF) is a hardware-based cryptographic primitive is proposed, that can track and identify an integrated circuit (IC). SDNs and Hardware based security solutions for IoT, though not fully explored, but are suitable candidates for securing IoT devices.

4. Discussion

IoT security is one of the key concerns that need to be catered to. In our article, we have reviewed some emerging technologies that promise a great deal in countering the different security issues. Fog computing reduces the burden of processing on both users as well as service levels. It provides a medium where multiple encryption algorithms can be utilized for IoT systems. Algorithms like ECDHE, multiple variants of Homomorphic encryption, and RSA can be integrated with IoT networks using the services of Fog and Edge layer. To counter centralized architecture failures, blockchain-based IoT systems promise decentralization, tamper resistance, and immutability. However, blockchain technology is still in its early stages of development. Hence, technical expertise is the requirement of the subject. Blockchain-based IoT systems have gained huge popularity due to various applications like food traceability and medical supply chain. Moreover, for such systems, scalability and privacy are the areas that need to be focused on in B-IoT systems. Utilization of possible scalable measures like sliding window protocol, EOG in litichain, and cloudlet technologies promise scalable and secure B-IoT systems. To tackle the attacks, devices trained with datasets of some commonly known attacks, hence can be detected in advance. In recent years there has been enormous growth in the development of IDS, that have reduced the probability of security attacks. Moreover, the development of federated learning promises sophisticated and secure IoT systems as training and learning can be utilized in a distributed manner. In this era of quantum computing, providing security to

TABLE III. Emerging security solutions in IoT using various domains

Group/Category	Reference	Contribution
Edge and Fog Computing	[21]	Proposed Fog based security solutions for smart grids and VANETS.
	[20]	Innovative security service Edge-Sec at edge layer.
	[22]	Proposed SIOTOME, a cooperative framework for real-time security.
	[23]	Programmable lightweight security architecture on edge computing.
	[24]	Proposed security framework based on network virtualization.
	[25]	Privacy preservation algorithms on Fog nodes using Homomorphic encryption.
	[26]	Data security utilizing Elliptic Curve Diffie–Hellman for IoT devices at Fog .
Blockchain	[27]	Possible mitigation strategies for IoT vulnerabilities by blockchain.
	[28]	Sliding window blockchain for securing IoT devices and blockchain scalability.
	[29]	Litichain, a scalable blockchain for securing IoT at Edge.
	[30]	Lightweight blockchain architecture with real-time encryption techniques.
	[31]	State of art of various blockchain-based security solutions for IoT.
	[32]	Summarizes the role of blockchain and ML in plugging IoT vulnerabilities.
	[33]	Proposes cloudlet technology in IoT and suggests the potential role of blockchain.
ML and DL	[34]	Prediction of unknown and mutant attacks using Deep Learning.
	[35]	Anomaly-based IDS deployed in real smart building scenarios.
	[37]	A wireless device recognition platform based on a deep learning approach.
	[38]	ML and DL-based systems that detect inhomogeneities in IoT networks.
	[39]	Deep learning-based IDS for malicious activities on IoT platforms.
	[40]	Federated approach combined with adaptable gradient descent.
Quantum Cryptography	[42]	Hybrid framework with quantum cryptography BB84 protocol.
	[43]	A broad overview of post-quantum IoT attacks and proposed solutions.
	[44]	Proposed quantum key (QDK) with RC6 that generates keys using photons.
	[45]	Bi-GISIS, a protocol using re-usable keys in multiple iterations.
	[46]	PQ-FLAT, Lattice-based cryptographic protocol for the post-quantum world.
Tiny Encryption	[47]	Enhanced TEA by rotating sub-keys in every round.
	[49]	Alteration to an original PRESENT cipher by lowering an encryption round.
	[50]	Proposed ETHASH, an enhanced version of original TEA.
	[51]	Dynamic Lightweight Symmetric encryption with XOR operator.
	[52]	Block cipher-based approach utilizing bitwise functions.
	[53]	IoT network with Enhanced security utilizing lightweight ECC.

a system is pretty difficult as it takes minutes to break a cipher which would otherwise require years. Development of Quantum resistant cryptographic techniques, especially LBE, BB84 protocol, and PQ-FLAT, are promising security solutions, especially for IoT-based systems. Another suitable technique for enhancing the security of IoT systems is TEA. DLS, modifications to PRESENT cipher, and proposed lightweight ECG solutions are some of the key solutions that have been discussed in the literature.

5. Future Research Direction

The previous discussion makes clear the critical role of mentioned technologies in securing IoT systems. Although we can move most operational procedures from IoT endpoints to the edge layer, many IoT systems still require a high level of data security for the communication channels that connect terminals to the edge. Blockchain integration in IoT needs more attention as there are multiple challenges of scalability and convergence. For Machine Learning based solutions, proper handling of training data sets is required. For utilizing ML in securing IoT data, more hybrid learning strategies and novel visualization techniques will suffice the need. However, the development of new AI approaches like Federated learning promises a great deal in enhancing the security of IoT devices. Federated approaches can collaborate with Fog computing to distribute the learning process and reduce the burden on centralized systems. The evolution of quantum computing is fast, so before devising any mechanism, even after proper analysis, we are unsure about its success. Also, Quantum computing algorithms require an enhanced skill set and resources at hand to implement in real-world scenarios. To implement TEAs in IoT systems, several challenges need to be addressed, and the algorithms need a slight modification for better adaptation In IoT systems.

6. Conclusion

IoT systems have gained rapid popularity over the past decade. However, these systems come up with a security challenge as they lack the proper infrastructure. The growth of emerging technologies like blockchain, Edge computing, Machine Learning, TEAs, and Quantum cryptography are promising solutions to these security challenges. There is still a need for optimization before converging any of these

technologies with IoT systems..

References

[1] J. Markarian, "Teris," Feb 2022. [Online]. Available: https://teris.com/interesting-2022-iot-statistics-and-how-it-applies-to-e-discovery/

[2] S. A. Al-Qaseemi, H. A. Almulhim, M. F. Almulhim, and S. R. Chaudhry, "Iot architecture challenges and issues: Lack of standardization," in *2016 Future technologies conference (FTC)*. IEEE, 2016, pp. 731–738.

[3] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "Iot: Internet of threats? a survey of practical security vulnerabilities in real iot devices," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8182–8201, 2019.

[4] Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, and S. Shieh, "Iot security: ongoing challenges and research opportunities," in *2014 IEEE 7th international conference on service-oriented computing and applications*. IEEE, 2014, pp. 230–234.

[5] J. H. Kong, L.-M. Ang, and K. P. Seng, "A comprehensive survey of modern symmetric cryptographic solutions for resource constrained environments," *Journal of Network and Computer Applications*, vol. 49, pp. 15–50, 2015.

[6] E. Leloglu, "A review of security concerns in internet of things," *Journal of Computer and Communications*, vol. 5, no. 1, pp. 121–136, 2016.

[7] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of things security: A survey," *Journal of Network and Computer Applications*, vol. 88, pp. 10–28, 2017.

[8] W. H. Hassan *et al.*, "Current research on internet of things (iot) security: A survey," *Computer networks*, vol. 148, pp. 283–294, 2019.

[9] D. Minoli and B. Occhiogrosso, "Blockchain mechanisms for iot security," *Internet of Things*, vol. 1, pp. 1–13, 2018.

[10] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on iot security: application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82 721–82 743, 2019.

[11] M. A. Amanullah, R. A. A. Habeeb, F. H. Nasaruddin, A. Gani, E. Ahmed, A. S. M. Nainar, N. M. Akim, and M. Imran, "Deep learning and big data technologies for iot security," *Computer Communications*, vol. 151, pp. 495–517, 2020.

[12] R. Asif, "Post-quantum cryptosystems for internet-of-things: a survey on lattice-based algorithms," *IoT*, vol. 2, no. 1, pp. 71–91, 2021.

[13] A. Attkan and V. Ranga, "Cyber-physical security for iot networks: a comprehensive review on traditional, blockchain and artificial intelligence based key-security," *Complex & Intelligent Systems*, pp. 1–33, 2022.

[14] M. Rana, Q. Mamun, and R. Islam, "Lightweight cryptography in iot networks: A survey," *Future Generation Computer Systems*, vol. 129, pp. 77–89, 2022.

[15] J. Fruhlinger, "The mirai botnet explained: How iot devices almost brought down the internet," Mar 2018. [Online]. Available: https://www.csoonline.com/article/3258748/the-mirai-almost-brought-down-the-internet.html

[16] D. Kushner, "The real story of stuxnet," Jul 2021. [Online]. Available: https://spectrum.ieee.org/the-real-story-of-stuxnet

[17] T. D. J. 20, T. D. , and A. Dunlap, "The 5 worst examples of iot hacking and vulnerabilities in recorded history," Mar 2022. [Online]. Available: https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities

[18] A. E. Montalbano and E. Montalbano, "Millions of routers, iot devices at risk from botenago malware." [Online]. Available: https://threatpost.com/routers-iot-open-source-malware

[19] M. Abdulraheem, J. B. Awotunde, R. G. Jimoh, and I. D. Oladipo, "An efficient lightweight cryptographic algorithm for iot security," in *International Conference on Information and Communication Technology and Applications*. Springer, 2020, pp. 444–456.

[20] K. Sha, R. Errabelly, W. Wei, T. A. Yang, and Z. Wang, "Edgesec: Design of an edge layer security service to enhance iot security," in *2017 IEEE 1st International Conference on Fog and Edge Computing (ICFEC)*. IEEE, 2017, pp. 81–88.

[21] A. Alrawais, A. Alhothaily, C. Hu, and X. Cheng, "Fog computing for the internet of things: Security and privacy issues," *IEEE Internet Computing*, vol. 21, no. 2, pp. 34–42, 2017.

[22] H. Haddadi, V. Christophides, R. Teixeira, K. Cho, S. Suzuki, and A. Perrig, "Siotome: An edge-isp collaborative architecture for iot security," *Proc. IoTSec*, 2018.

[23] R.-H. Hsu, J. Lee, T. Q. Quek, and J.-C. Chen, "Reconfigurable security: Edge-computing-based framework for iot," *IEEE Network*, vol. 32, no. 5, pp. 92–99, 2018.

[24] P. Zhang, C. Jiang, X. Pang, and Y. Qian, "Stec-iot: A security tactic by virtualizing edge computing on iot," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2459–2467, 2020.

[25] A. Murugesan, B. Saminathan, F. Al-Turjman, and R. L. Kumar, "Analysis on homomorphic technique for data security in fog computing," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 9, p. e3990, 2021.

[26] S. Amanlou, M. K. Hasan, and K. A. A. Bakar, "Lightweight and secure authentication scheme for iot network based on publish–subscribe fog computing model," *Computer Networks*, vol. 199, p. 108465, 2021.

[27] J. Sengupta, S. Ruj, and S. D. Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for iot and iiot," *Journal of Network and Computer Applications*, vol. 149, p. 102481, 2020.

[28] P. Koshy, S. Babu, and B. Manoj, "Sliding window blockchain architecture for internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3338–3348, 2020.

[29] C. K. Pyoung and S. J. Baek, "Blockchain of finite-lifetime blocks with applications to edge-based iot," *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 2102–2116, 2019.

[30] S. Latif, Z. Idrees, J. Ahmad, L. Zheng, and Z. Zou, "A blockchain-based architecture for secure and trustworthy operations in the

industrial internet of things," *Journal of Industrial Information Integration*, vol. 21, p. 100190, 2021.

[31] B. Bhushan, C. Sahoo, P. Sinha, and A. Khamparia, "Unification of blockchain and internet of things (biot): requirements, working model, challenges and future directions," *Wireless Networks*, vol. 27, no. 1, pp. 55–90, 2021.

[32] O. Alfandi, S. Khanji, L. Ahmad, and A. Khattak, "A survey on boosting iot security and privacy through blockchain," *Cluster Computing*, vol. 24, no. 1, pp. 37–55, 2021.

[33] A. Al Sadawi, M. S. Hassan, and M. Ndiaye, "A survey on the integration of blockchain with iot to enhance performance and eliminate challenges," *IEEE Access*, vol. 9, pp. 54 478–54 497, 2021.

[34] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for internet of things (iot) security," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1646–1685, 2020.

[35] H. Hindy, R. Atkinson, C. Tachtatzis, J.-N. Colin, E. Bayne, and X. Bellekens, "Utilising deep learning techniques for effective zero-day attack detection," *Electronics*, vol. 9, no. 10, p. 1684, 2020.

[36] M. Bagaa, T. Taleb, J. B. Bernabe, and A. Skarmeta, "A machine learning security framework for iot systems," *IEEE Access*, vol. 8, pp. 114 066–114 077, 2020.

[37] H. Jafari, O. Omotere, D. Adesina, H.-H. Wu, and L. Qian, "Iot devices fingerprinting using deep learning," in *MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM)*. IEEE, 2018, pp. 1–9.

[38] S. Roy, J. Li, B.-J. Choi, and Y. Bai, "A lightweight supervised intrusion detection mechanism for iot networks," *Future Generation Computer Systems*, vol. 127, pp. 276–285, 2022.

[39] S. Panja, K. Yadav, and A. Nag, "Anomaly detection at the iot edge in iot-based smart home environment using deep learning," in *Proceedings of International Conference on Advanced Computing Applications*. Springer, 2022, pp. 119–125.

[40] X. Wu, Y. Zhang, M. Shi, P. Li, R. Li, and N. N. Xiong, "An adaptive federated learning scheme with differential privacy preserving," *Future Generation Computer Systems*, vol. 127, pp. 362–372, 2022.

[41] A. Khalid, S. McCarthy, M. O'Neill, and W. Liu, "Lattice-based cryptography for iot in a quantum world: Are we ready?" in *2019 IEEE 8th International Workshop on Advances in Sensors and Interfaces (IWASI)*. IEEE, 2019, pp. 194–199.

[42] A. Lohachab, A. Lohachab, and A. Jangra, "A comprehensive survey of prominent cryptographic aspects for securing communication in post-quantum iot networks," *Internet of Things*, vol. 9, p. 100174, 2020.

[43] J. Krämer, "Post-quantum cryptography and its application to the iot," *Informatik Spektrum*, vol. 42, no. 5, pp. 343–344, 2019.

[44] Z. A. Abdulkader *et al.*, "A secure iot system using quantum cryptography with block cipher," *Journal of Applied Science and Engineering*, vol. 24, no. 5, pp. 771–776, 2021.

[45] K. Seyhan, T. N. Nguyen, S. Akleylek, K. Cengiz, and S. H. Islam, "Bi-gisis ke: Modified key exchange protocol with reusable keys for iot security," *Journal of Information Security and Applications*, vol. 58, p. 102788, 2021.

[46] E. Karacan, S. Akleylek, and A. Karakaya, "Pq-flat: A new quantum-resistant and lightweight authentication approach for m2m devices," in *2021 9th International Symposium on Digital Forensics and Security (ISDFS)*. IEEE, 2021, pp. 1–5.

[47] R. M. De Leon, A. M. Sison, and R. P. Medina, "A modified tiny encryption algorithm using key rotation to enhance data security for internet of things," in *2019 International Conference on Information and Communications Technology (ICOIACT)*. IEEE, 2019, pp. 56–60.

[48] C. K. Rajak and A. Mishra, "Implementation of modified tea to enhance security," in *International Conference on Information and Communication Technology for Intelligent Systems*. Springer, 2017, pp. 373–383.

[49] R. Chatterjee and R. Chakraborty, "A modified lightweight present cipher for iot security," in *2020 International Conference on Computer Science, Engineering and Applications (ICCSEA)*. IEEE, 2020, pp. 1–6.

[50] O. R. Oluwade, O. M. Olaniyi, Y. S. Abdulsalam, L. A. Ajao, and F. B. Osang, "Eteash-an enhanced tiny encryption algorithm for secured smart home," 2021.

[51] S. Banani, S. Thiemjarus, K. Wongthavarawat, and N. Ounanong, "A dynamic light-weight symmetric encryption algorithm for secure data transmission via ble beacons," *Journal of Sensor and Actuator Networks*, vol. 11, no. 1, p. 2, 2022.

[52] M. K. Nayak and P. K. Swain, "Esit: An enhanced lightweight algorithm for secure internet of things," in *IoT and Analytics for Sensor Networks*. Springer, 2022, pp. 107–116.

[53] T. Islam, R. A. Youki, B. R. Chowdhury, and A. Hasan, "An ecc based secure communication protocol for resource constraints iot devices in smart home," in *Proceedings of the International Conference on Big Data, IoT, and Machine Learning*. Springer, 2022, pp. 431–444.

[54] C. Gonzalez, S. M. Charfadine, O. Flauzac, and F. Nolot, "Sdn-based security framework for the iot in distributed grid," in *2016 international multidisciplinary conference on computer and energy science (SpliTech)*. IEEE, 2016, pp. 1–5.

[55] W. Liu, L. Zhang, Z. Zhang, C. Gu, C. Wang, M. O'neill, and F. Lombardi, "Xor-based low-cost reconfigurable pufs for iot security," *ACM Transactions on Embedded Computing Systems (TECS)*, vol. 18, no. 3, pp. 1–21, 2019.

Iraq A Reshi Iraq A. Reshi is a Research Scholar at department of Computer Science Engineering, Islamic University of Science and Technology Awantipora, Pulwama , JK, India . He has pursued his B.Tech from National Institute of Technology Srinagar, India, and M.Tech from Central University of Kashmir, India. His research focuses on Security, Blockchain, and Internet of Things.

Sahil Sholla Sahil Sholla Sahil Sholla, is Assistant Professor at department of Computer Science Engineering, Islamic University of Science and Technology Awantipora, Pulwama, JK, India .He has received PhD from National Institute of Technology Srinagar, India. His research focuses on technology ethics, security,Blockchain and Internet of Things.