Vol. 2 No. 3 (2024)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138
Print ISSN
3007-312X

An Efficient Artificial Intelligence (AI) and Blockchain-Based Security Strategies for Enhancing the Protection of Low-Power IoT Devices in 5G Networks

Ibrahim Akmal[1]
Department of Computer Science, Faculty of Computer Science & IT
Superior University Lahore, 54000, Pakistan
ibrahimakmal9797@gmail.com

Hamayun Khan[2]
Department of Computer Science, Faculty of Computer Science & IT
Superior University Lahore, 54000, Pakistan
hamayun.khan@superior.edu.pk

Ayesha Khushnood[3]
Department of Computer Science, Faculty of Computer Science & IT
Superior University Lahore, 54000, Pakistan
ayeshakhushnood6@gmail.com

Fatima Zulfiqar[4]
Department of Computer Science, Faculty of Computer Science & IT
Superior University Lahore, 54000, Pakistan
fzulfiqar860@gmail.com

Eman Shahbaz[5]
Department of Computer Science, Faculty of Computer Science & IT
Superior University Lahore, 54000, Pakistan
emanshahbaze@gmail.com

Abstract

Today, the ever-growing Internet of Things revolutionizes the face of digital connectivity. IoT devices are proliferating while 5G networks are constantly being deployed all over the world. All these new developments bring the problem of privacy concern for these low consumption, less computational IoT devices. This paper details an advanced security framework for the protection of those devices by integrating AI and blockchain but in focus on real-time anomaly detection and decentralized data integrity. This research will employ systematic literature review to determine the current solutions that reveal AI-based solutions for network anomaly detection and blockchain to secure data without central control. It will adapt AI to ensure the best threat detection and protection through blockchain for the best possible protection of data against attacks like unauthorized access and DDoS attacks. The combination of AI and blockchain seems to represent a good solution for 5G securing the Internet of Things by creating a balance between protecting data and energy efficiency. The limits of the power of computational devices indicate further refinements in these technologies at scale. The future agenda of research should target at reducing the computational demands along with standards to be created for unified IoT security. Therefore, the frameworks compared in this paper review is efficient and secure in supporting a future-proof 5G-ready IoT ecosystem against emerging threats and supports high interconnectivity

Keywords: IoT devices, Networking, 5G, AI, blockchain, low-power IoT devices, decentralized security, Blockchain.

Introduction

Internet of Things (IoT) was primarily introduced in 1999[i]; The idea of IoT revolves around the word intelligence which means a quality to independently acquire and implement knowledge.[ii] In fact, the topic is only gaining momentum since that time with the advent and proliferation of M2M. Smartness comes in combination with IoT, that is a feature of devices capable of both applying and gaining knowledge automatically. Atzoriet al.[iii]envision IoT from three perspectives - an Internet-Oriented view (emphasizes connectivity), Things-Oriented one (focus on things) and Knowledge-Orienting view. ITU perspective is along those lines, where everything gets connected. However, it should be as transparent & unobtrusive in the user experience when handling smart objects as possible.[ivv]

The Internet of Things (IoT) has changed our way of living, bringing in numerous applications and services previously impossible few years back. This means that IoT ecosystem is expected to be an essential stack in the future 5G framework. Yet until those revolutionary systems are fully matured and realized, a great deal of activity is aimed at squaring the security holes in the innovative 5G design. This sets the scenario for our lives to become more intertwined as these technologies converge, bringing with it issues related security and privacy.[vivii]

Over the last decade, several other products have been developed in most parts of the world, categorized under the name of IoT. Unimaginable close to 15 billion Devices Networks Connected Physically means nearly two devices per individual in earth.[viii] And that the trend continues as, according to various forecasts by different research institutions, close to 26 billion will be connected by 2020. Most of them are IoT and wearables[ix]. Most things probably by 2025 would have Internet nodes embedded within them; this will multiply the numbers of internet-enabled devices considerably.[x] Cisco suggests that there will be roughly 500 billion devices which will be available on the internet until the year

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN 3007-3138
Print ISSN 3007-312X

2030. In like manner in 2013, Telefonica had indicated that in 2020, out of ten, one car will not be on the Internet.[xi]

According to Ericsson's estimate [xii], there are expected to be approximately 28 billion connected smart devices worldwide by 2021, with greater than 15 billion of them expected to be linked to electricity from M2M. The research also suggests that approximately 7 billion of these devices will be engaged with mobile networks such as 2G, 3G and 4G. With the use of multi-area network (LPWA) technology,[xiii] the entire global IoT space will generate an income of approximately 4.3 trillion US dollars. [xiv]. The current demands for technology-based communication (MTC), such as intelligent communities [xv], intelligent buildings and monitoring [xvi], intelligent cities [xvii], intelligent projects [xviii], far-end maintenance and monitoring [xix], as well as intelligent water equipment [xx], etc., have brought about many connected devices that will affect the current transmission capacity and future communication capacity.

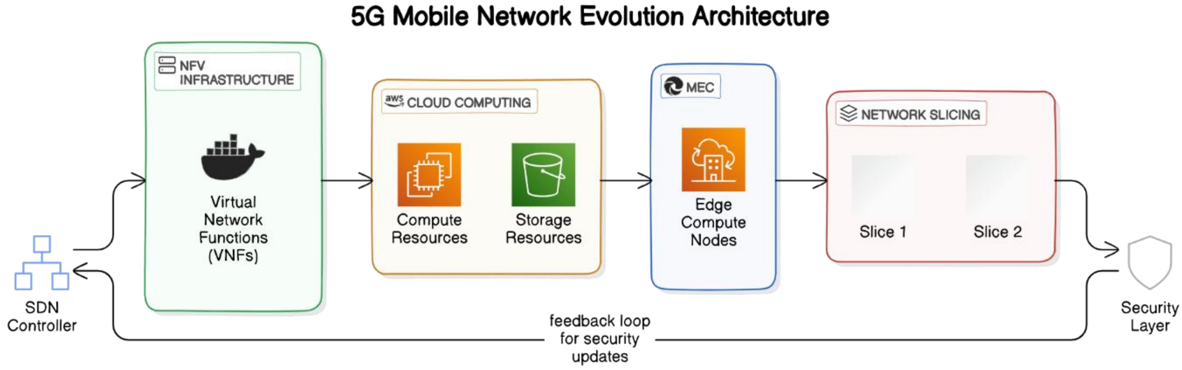

Fig. 1. 5G mobile network evolution architecture

The aim of mobile network evolution is towards the new requirement of network services, mainly to advance in terms of performance and flexibility, with portability and energy efficiency. The implementation of 5G introduces new principles for networking

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

while improving on aspects like that[xxi]. The pace at which the telecom standards organization is integrating novel concepts into telecommunication networks is rapidly evolving,[xxii] [xxiii] such as integrating concepts like SDN, NFV, cloud computing, MEC, and NS. (NS).[xxiv] All these should be developed with a new, software-driven mobile network that will meet the needs of developing services for the future.

SDN introduces the separation of control and data planes in network devices. Centralization of network intelligence in a single controller allows this setup to provide an abstract view of the network infrastructure for both control and application layers. NFV brings a new approach towards creation, deployment, and management of network functions detaching them from dedicated hardware that run as software-based instances. Cloud computing and MEC offer scalable, on-demand resources to the network; Network Slicing would support a myriad of traffic types in a 5G environment, but security and protection of privacy become concerns as attacks at vulnerabilities can cause catastrophic failures.[xxv]

The new wireless communication systems have emerged as a base for many applications beyond just voice calls, including games, online shopping, social networking, BYOD, smart home integration, and cloud services, which is the new challenge to the developers to solve [xxvi] [xxvii]. Phreaking, which initially targeted general data theft, has become major cybercrime operations due to financial, political, and personal interests [xxviii] [xxix]. Additionally, with the increase in IoTs, 5G also faces different types of vulnerabilities [xxx].

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Today, IoT devices are deployed in various environments [xxxi].IP cameras are being used by the police and customs to capture biometric details for the prevention of crime and to make sure that immigration of people becomes smooth [xxxii]. National aviation safety authorities use GPS sensors to monitor airplanes to ensure greater safety and emergency reaction times [xxxiii]. IoT has also been applied in primary production for agriculture progress. This intrusion of privacy and security goes past the activities directly carried out through a device in the daily life and talk, especially for the smart speaker and IP cameras which are constantly on [xxxiv]. This goes beyond that, data collected through such devices could never have agreed to some people involved with them perhaps safe [xxxv].

Having intelligent speakers, toys, cameras, introduces privacy and security concerns over the direct use of these tools to invade the lives and conversations of those who live alongside them. For example, always-on devices such as smart speakers and IP cameras are not exempt [xxxvi]. Moreover, the data from these devices might not be knowingly shared by users, nor properly kept [xxxvii]. This is very scary for smart toys because, by design, they intend to target children as main users. The case for the Fisher Price Bear was an intelligent device meant to be used interactively during play. This was infiltrated by cybercriminals. The research established vulnerabilities in the toy's various communication technologies and sensors-including a nose camera-through which unauthorized users might gain a root access into the gadget [xxxviii]. Although this problem is a typical threat to IoT devices, it is also known that even the most common household appliances share similar security weaknesses [xxxix] [xl].

Researches till now predict that the increased of security features in 5G networks can greatly decrease invalidate access and potential utilization [xli]. Future work can be focused on designing better and more efficient malware detection mechanisms. Most of the proposed solutions for securing 5G have not been tested on a large scale in real field environments and implemented on a wide scale, thereby achieving as much protection as possible. The developments in artificial intelligence and. Other advanced technologies including Internet of Things; blockchain and cloud computing and many more can be provided with additional security by means of 5G.ML is often proposed together with AI to fortify the security of IoT devices mainly because it is deployed at the network edge [xlii] [xliii] [xliv]. The most significant drawbacks of ML in improving security and privacy are that attackers can exploit the same and bypass the protection mechanisms [xlv].

Machine learning (ML) is heavily applied in day-to-day life for improving the online security and privacy aspects. ML refers to developing an algorithm which learns with experience over given data and predicts new events on statistical patterns [xlvi] [xlvii]It has a set of predefined rules which need to work to combat cybercrime by using ML. The set of rules allows ML to make real-time decisions that make security and privacy enhanced. An example would be emailing spam filtering. In this case, an email provider or user may set rules like a specific subject lines, hostnames email address, , key terms, IP addresses, to be used by an email spam filter within an algorithm in detecting and blocking unwanted messages [xlviii]. Although the underlying technology would be different in an IoT, application of ML to secure an IoT device is basically the same in concept. Filters can be defined using rules that augment real-time security of the device without explicit programming.

AI is one of the major technologies in the defense side of cybersecurity. As per the survey by Capgemini Research Institute, 69 percent of 850 senior IT executives said AI would let them respond more effectively to cyberattacks, and 61 percent said AI was required for threat detection [xlix] [l]. The capability of AI to operate without being administered by a human makes it one of the strongest advantages in the context of cybersecurity [li]. AI computes tasks in such a way done by humans it makes decision in almost the same way as humans do as it is made on the same mechanism of human neurons. It stores data in form of matrices and it copies human way of making decisions in an organized manner[lii].

Prior Research

History in Mobile Network Security and Emerging Threats

In fact, different types of wireless systems were adopted by diverse IoT systems, namely 2G, 3G or 4G, and so forth and 5G which is being implemented for billions of connections. Below lets evaluate the security feature and drawbacks of these systems:

1G Security Environment and Weaknesses:

In the 1980s, 1G networks were analog and merely offered simple voice services with no provision for data and roaming services [liii]. Their security was very basic. As encryption was unheard of at that time, calls could easily be tapped. Mobile Identification Numbers (MIN) and Electronic Serial Numbers (ESN) could be obtained using radio scanners, thus making it relatively easy to clone phones [liv]. More advanced versions offered analog scrambling but nothing more advanced than that which is used in later generations with high-grade encryption.

2G Security Features and Challenges:

2G networks were digitized technologies launched in 1991, which introduced SMS services for voice and messaging. Improvements included subscriber authentication, radio interface encryption, and SIM cards for subscriber identity verification. However, vulnerabilities such as spam attacks and weaknesses in A5/1 and A5/2 encryption expose the 2G networks to real-time ciphertext-only attacks. Moreover, the basic nature of roaming SMS, which is to store and forward, exposes them to external internet threats.

3G Security Model and Threat Mitigations:

Mobile data applications and internet access entered with the release of 3G back in 2001. Many of the previously existing flaws were successfully dealt with it, while other new things in security architecture were found to be access security and domain security with improved protection of applications with measures towards preventing false base station attack and increasing length of key. Despite the above considerations, 3G Networks still presented threat to both users and network in regards to eavesdropping along with man-in-the-middle attacks for user and network authentication.

4G Security Model and Threat Mitigations:

4G LTE primarily came into practice in 2010 for mobile networks with an end-to-end all-IP architecture which provides speeds of up to 100 Mbps. Here, advanced cryptography algorithms EEA and EIA emerged as EPS encryption algorithms with key sizes as large as 256 bits, so security strength is almost double from what was established in its predecessors, that is 3G [lv]. Moreover, 4G networks had introduced the AKA protocol, which was based on NAS and RRC signaling for replay and integrity protection of the authentication message. The 4G backhaul traffic was also encrypted with IPsec[lvi lvii].

This open IP architecture made 4G networks more vulnerable to various threats originating from the Internet such as IP address spoofing, TCP SYN DoS, user ID theft, and many other forms of denial-of-service attacks [lviii lix]. Unlike previous non-IP protocols, the IP core of 4G made the process of understanding and exploitation by attackers much easier [lx lxi]. It also paved the way for botnet and APT attacks by high-powered 4G devices, and vulnerabilities through non-3GPP networks like Wi-Fi and WIMAX are brought in due to the fact that they have an inherently lower security level. The main challenge is DDoS attacks; they still bring financial loss and a new problem for detection in the IP-based environment.[lxii]

Privacy features and issues in 5g network:

5G networks envision smart services to the end-users, which pose remarkable privacy concerns since such smart services involve sensitive user data that includes identity, location, and private details. Because of the handling and access provided by multiple stakeholders on these data, leakage of private data is a serious problem. This section focuses on user-centric privacy categories, specific privacy concerns related to 5G networks, and privacy objectives based on the 5G architecture. From the perspective of cloud computing, it seems hard to address all such privacy concerns for stakeholders of 5G since 5G is huge in scope and involves all possible stakeholders, technologies, businesses, and regulations, hence complex in nature. Technologies such as SDN and NFV relate closely to the cloud perspective as well.

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN 3007-3138
Print ISSN 3007-312X

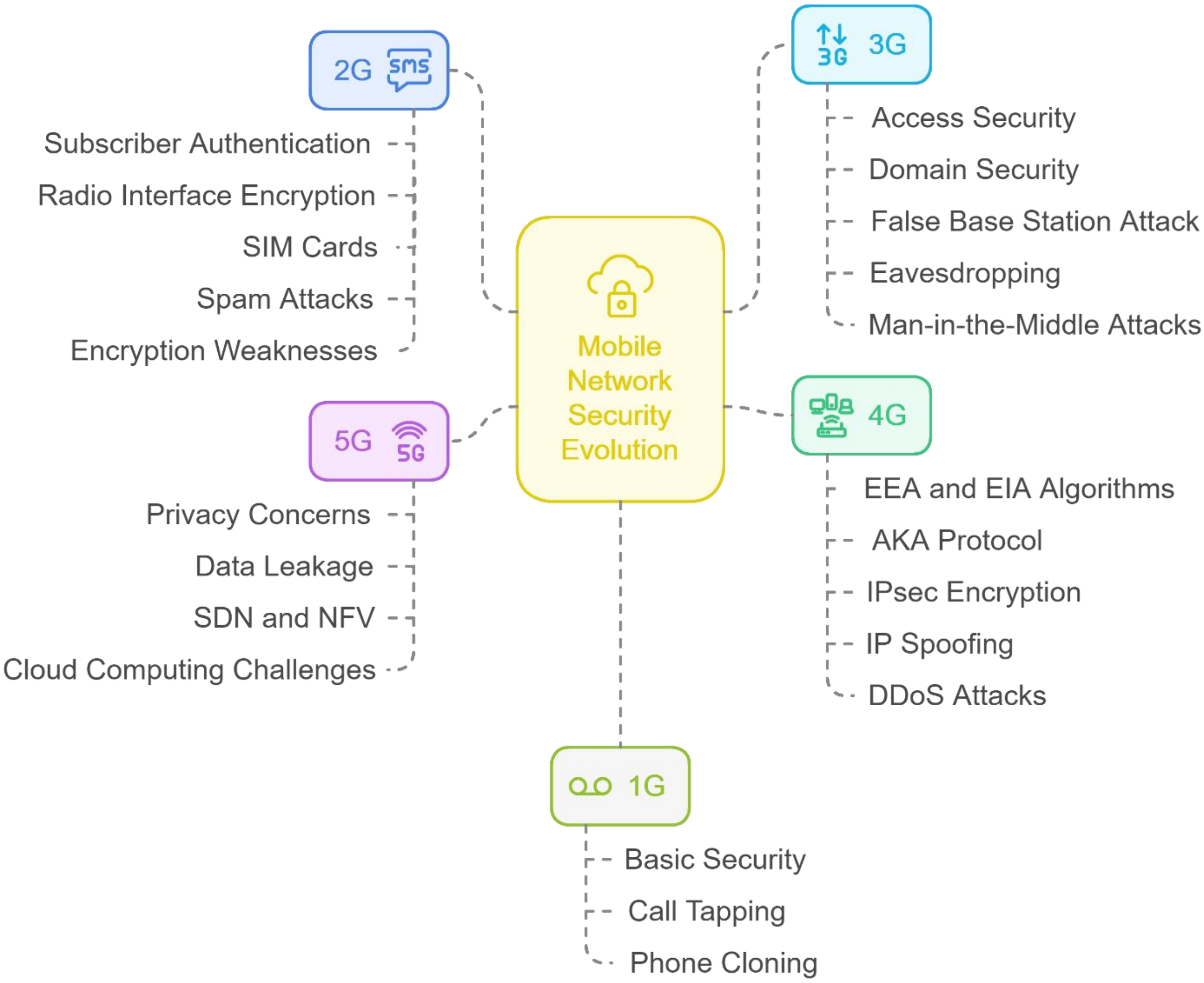

Fig. 2 Mobile Network Security Evolution from 1G to 5G

Amongst systematic literature review, which one of the most up to date has been recently undertaken as back return by Bacca and Kitchenham [lxiii] by Torres Carrin [lxiv] focusing on analyzing in deepness issues related with security features networks. The paper is based on the planning and reviewing of a few issues and privacy concerns that affect the performance of the networks and the basis of security.

Q. Tang [lxv], has in his paper, precisely explained the features of the 5G and furthermore, about the network's security. He even specified how the issues of IoT could be resolved with network technologies (IoT). Thus, the aim of research for this, a methodology has to be developed that can be use to protect the LTE advanced network. Author Ahmad I. studied different types of attacks and security issues that are encountered in networks. He further discussed the different security measures that the industry has adopted to curb the issues. Some of these are the 3GPP, 5GPPP, and the Internet Engineering Task Force [lxvi].

Referencing A. Dutta's study on "5G Security Challenges and Opportunities," [lxvii]. He provided further discussion over a lot of facets that entail security-related issues along with directions into the future threat that will evolve on its standards. How such progress has already been misused in industries. It described how such various aspects in it that constitute its safety will unfold toward the future. Many studies in reference to aspects related to this type of security of 5G. Over the past years the of work on the technology has increased drastically. It is also envisaged that the researches on the security of network will rise in 2022[lxviii].

As the authors pointed out,[lxix], the future of next-generation wireless networks will be based on integration of connected intelligence within communication systems, together with advancement in networking and AI technologies. [lxx]. Furthermore, the authors in [lxxi] state that the increased speed and lower latency would be sufficient to allow the usage of already increasing technologies like the wearable IoT devices and autonomous vehicles The authors expect that future networks will provide 3D holographic projections of personal models for virtual meetings along with fused reality, physical internet, and embedded devices. Most of the possible applications of the next generation networks researched are not IoT dependent but nearly all integrate or are affiliated with the IoT industry. Based on this, authors of it have shown that one of the primary visions of 6G as an emerging potential future a standalone network, which is actually just how IoT works. Although, as the authors in [lxxii] and explain, there are security as well as privacy concerns regarding a futuristic 6G network and IoT that current researchers are exploring into that will be affecting security of the visions introduced.

In addition to being crowded on the existing networks due to network congestion, what is needed for faster telecommunication transmission includes of data with lower latency that was identified as early as 2015 [lxxiii] [lxxiv] [lxxv]. Low latency and better performance became a necessity of IoT in industrial scenarios. Later the same has been supported in the year 2017, by the authors of reference. With all research on the improvement in latency and overall performance within existing 5G network infrastructures [lxxvi] the present-day networks start looking insufficient to meet their performance requirements in terms of data communication from IoT applications. The congestion will continue to degrade the already slow transmission, further delaying latency on existing networks.

In future networks like 6G, blockchain and AI will be crucial to upgrade both security and operational capacities. The full automation capability of 6G relies on AI, especially with regard to intelligent edge computing, optimal resource management, and further refinement of identifying users. However, new security vulnerabilities will be dependent on the reliance on AI, attacking AI to undermine network functionalities and data privacy.

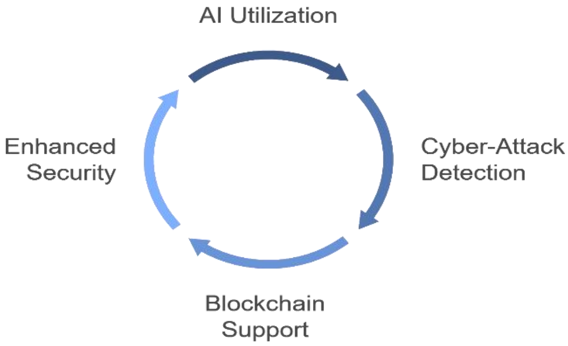

Fig. 3. AI-Driven Security Cycle

Blockchain will support AI as it encompasses methods AI utilizes in terms of detecting and preventing types of blockchain attacks, specifically 51% attacks; thus, when integrated with this technology, the resistance against cyber threats in the network will be stronger. Figure 3 In this way, AI can be used for the cyber-attack detection that serves as feedback into the improvements of blockchain security. An adaptive, robust security mechanism is therefore brought about through this cycle of cyberattack detection and AI-based responses to these cyberattacks contributing toward a better security infrastructure for the network as such.

Increasing Internet of Things devices demand new network architectures in order to handle the amount of bandwidth these devices would require at unprecedented speeds. So much research is being invested in this area today focusing on 6G and data communication but yet there is much to be uncovered about privacy and security issues. While discussions about AI, machine learning, and blockchain still continue, it is specifically the physical layer of the IoT infrastructure that poses vulnerable security threats. Strengthening these issues of which some have latency relations will be pivotal to enabling secure future networks. So, the next study could be aimed at developing strengthening in the physical

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN 3007-3138
Print ISSN 3007-312X

layer of this advanced network that ensures even greater security on upcoming new networks.

Major Contributions

Grounded on the discussed major challenges. The major participation of this research is below:

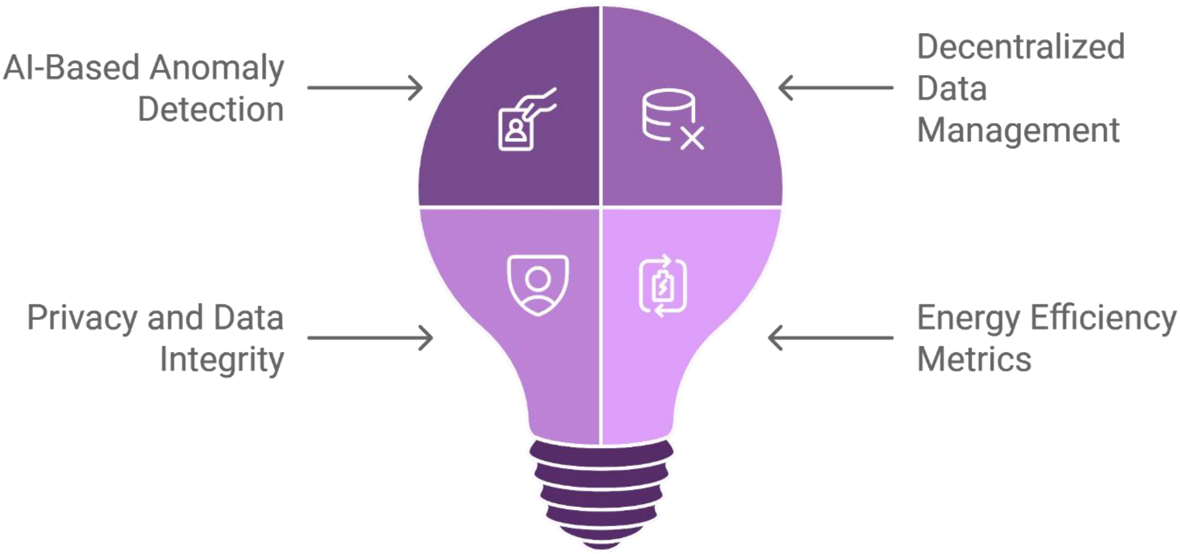
AI-Based Anomaly Detection
Decentralized Data Management
Privacy and Data Integrity
Energy Efficiency Metrics

Fig. 4. Exploring AI and Blockchain Innovation

AI-Based Anomaly Detection: Through this paper, it can be concluded that AI-based approaches and anomaly detection more specifically have dramatically improved real-time accuracy of threat detection from low-power IoT devices operating in 5G networks.

Decentralized Data Management: It is basically about the use of blockchain technology for providing decentralized energy-efficient data security to the IoT devices that makes it better than
a central authority.

AI and Blockchain: The paper discusses AI in the context of blockchain as a way of balancing the security with energy efficiency

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN 3007-3138
Print ISSN 3007-312X

while hinting towards low-power approaches such as Proof-of-Enough-Work (PoEW) and Lightweight DAG structures.

These identify real risks such as restricted access and Distributed Denial of Service attacks that will be best mitigated with the application of AI and blockchain technologies within IoT networks.

Privacy and Data Integrity: This paper has illustrated how the integration of AI and blockchain improves the user's privacy and data integrity in smart IoT applications so that users have greater control over their data.

Energy Efficiency Metrics: It thus provides central metrics of energy efficiency on AI-blockchain security systems for the balance between security and minimal energy use.

Research Questions:

To what extent can AI anomaly-based detection contribute to online threats for 5G, Low-power IoT devices2. How do the blockchains aid in the design of decentralized energy-efficient mechanisms for IoT data security for the 5G scale?

- Up to what extent the balance between hybrid AI and Blockchain balance security and energy efficiency in Low-power IoT can be?

Which of the above threat through the 5G IoT is best to address via AI/Blockchain?

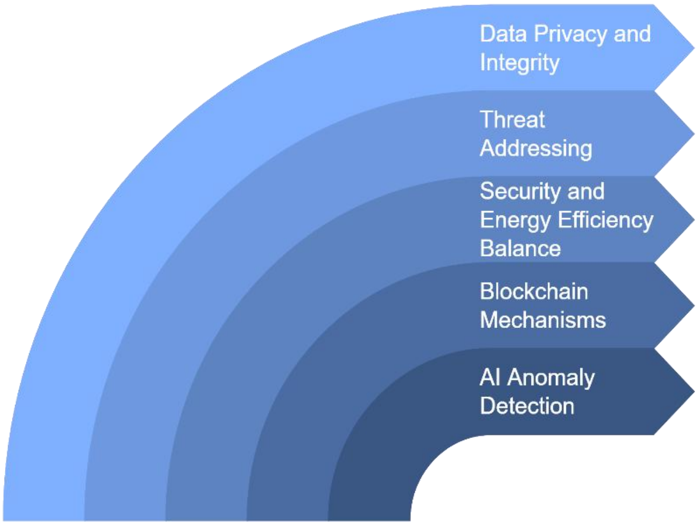
Data Privacy and Integrity
Threat Addressing
Security and Energy Efficiency Balance
Blockchain Mechanisms
AI Anomaly Detection

Fig. 5. Enhancing Security with AI and Blockchain

- Is it safe or detrimental to smart IoT applications data privacy/integrity if AI blockchain has a deeper integration?

- What are most related metrics which can measure assessments on the energy efficiency on AI blockchain security pertaining over IoT?

Methodology:

This paper uses the methodology of a literature review to examine the dominant security threats to personal IoT devices in 5G networks, 5GBN. This literature review will identify the existing privacy challenges, possible solutions, and areas of future work. The methodology includes well-defined criteria for inclusion and exclusion into the selection of a database and application of the emergent technologies- AI, ML, and blockchain to the comprehensive analysis of risk against security protection of IoT within 5G networks.

Exclusions criteria

After determining the research area, specific inclusion and exclusion criteria were developed to guide the selection of articles in this study. Such criteria keep the research focused and pertinent to the topic at hand. Moreover, they are useful in the formulation of appropriate search terms to be used in the searching of databases for relevant literature. The exclusion criteria are as follows with brief descriptions for each:

- Knowing well the fact that the IoT industry grew rapidly, this study narrowed its scope of study and limited its use of articles written after 2009. Although the term "IoT" was coined ages before the selection period began, research also showed the adoption rate of IoT devices also started booming between 2008 and 2009, when it hit the global population of interconnected devices. It was third-generation (3G) wireless technology in 2009, which made it history as IoT went mainstream for a wider population. Since 3G is phasing out, with 5G launched only in 2019, the focus on this period ensures that the research would cover modern IoT developments relevant to today's technological landscape.

- Since this research is more focused on 5G-enabled IoT networks, the current technologies such as 4G and legacy systems are out of the picture so as to keep focus only on the specific security consideration as well as capabilities within a 5G network.
- It's like personal and industrial IoT applications belong to the same characteristics as it mainly emphasizes the security application of personal IoT devices. Based on their privacy, security, and usability issues, personal IoT devices are separated from the industrial application of the IoT devices.
- Legislation does touch on parts of IoT security and privacy; however, the actual research covered here does not look at legislation or any other legal obligations associated with the use of IoT or the communications of networks. The focus here is rather much more on technical solutions applied to security and privacy concerning personal usage with devices featuring IoT, not concerns to state-specific compliance requirements nor even international regulatory obligations.

Inclusions criteria:

Below is a list of the inclusion criteria that makes an in-depth analysis of the research questions articulated.

- User-centric problem Since identified significant security challenge for IoT data results from the use of low-power IoT Devices by users, there is a need to study the role of individual users.

- Contemporary computer technologies. Since the increasing use of contemporary technologies is based on blockchain, AI, and ML, it logically follows that such technologies ought not to be excluded simply to determine how those technologies can be used constructively to improve protection and vulnerabilities that can be identified based on their use.
- Sensitivity and privacy of the data of IoT devices Since the paper to be reviewed addresses data privacy and sensitivity of the IoT devices over 5GBN, this also calls for embedding within the Character of IoT. Since it is their characteristics that one of the key reasons through which IoT devices are violated, then there is a need to embed the characteristics of IoT.
- The 5G networks beyond. While researchers are already studying the applications related to 5G, studies on networks further ahead are pretty basic already in progress.
- Security protocols for personal IoT devices: These are security protocols developed to enhance the safety of products, services, and systems through clear specifications, procedures, and best practices. Security protocols for personal IoT devices will be analyzed to point out specific areas that need improvement.

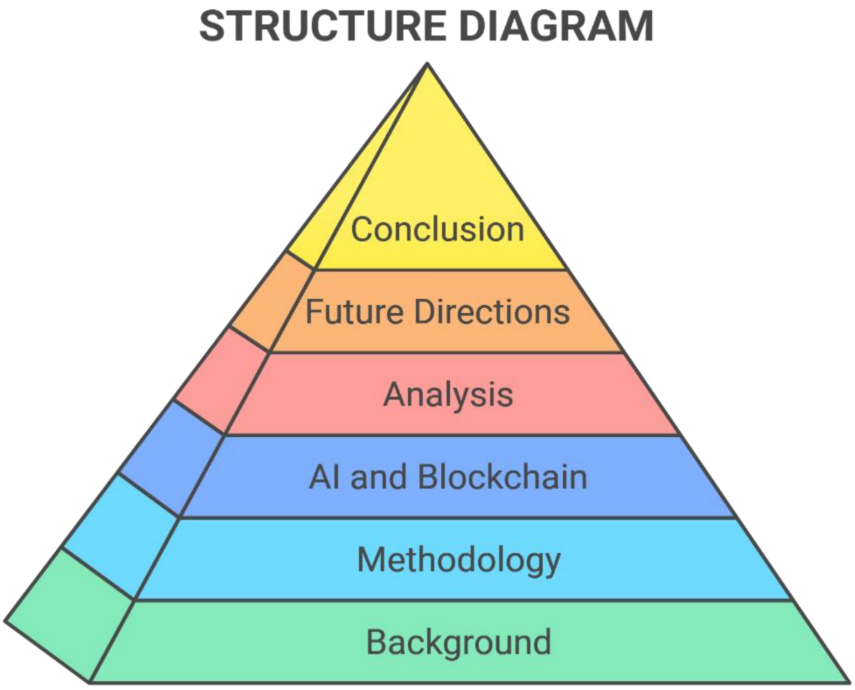

Fig. 6 Outline of Paper

Database selection and Search strategy:

A thorough literature search was done for proper identification of the research questions. Since the inclusion and exclusion criteria had been outlined above, the focused publication search was for the year of publication 2005-2023.However journal articles that had been printed and disseminated since as far back as 1989 were also included to help with the provision of pertinent history regarding internet privacy an indispensable aspect of IoT privacy Google Scholar, IEEE Xplore, and Scopus was applied to identify the thematic trend of articles picked from these periods. I sourced the titles, keywords, and abstracts of these shortlisted papers for them to be analyzed thematically. From my search, I narrowed down to an article list of 60; most relevant ones of these are summarized in Table.

Table 1. Related literature

Publications	Methodology	Strength	Limitations	Future Work
lxxvii	Review of current privacy and security measures.	It gives a comprehensive analysis of the current protocols.	Difficult to adapt to the intricate IoT landscape.	Proposes future research on energy-efficient, low-latency security methods.
lxxviii	Risk assessment and framework proposal for improved security.	In-depth analysis of risks and framework enhancement.	Limited to existing network technologies.	Suggests cryptographic solutions for efficient, standardized data collection.
lxxix	Extensive study of the 5G architectures such as Small Cells, D2D communication and	It delivers in-depth analysis on how the networks scale and adapt to the dynamic	It still faces challenges to achieve no interference and cost-effectiveness in deployments while staying	It shall be able to cater to further research on how scalable solutions can be realized

	Cognitive Radio Networks that maximize connectivity and efficiency.	changes, and pace with the high demand for data.	safe and secure.	energy-efficiently with special focus on frameworks which must support security robustly across the dense network environments.
lxxx	A systematic approach is developed by dividing the attacks into categories of objectives, proposed countermeasures, reasons, and root causes, and this approach is	It provides an exhaustive analysis of the security of mobile networks by tracing trends in attack vectors and comparing them with existing defenses to	The methodology may not be robust enough to address the sophisticated and dynamic nature of threats posed by 5G, especially with new tactics of attack and	This pre-authentication traffic security, mitigation of downgrade attacks, strengthening inter-operator protocols, and designing protocols

	applied to the literature of security issues in all three generations of mobile.	highlight gaps for future research.	the complex IoT system.	resistant to DoS attacks are proposed.
lxxxi	Probabilistic security technique-based experimental approach for IoT.	Points out vulnerabilities largely against man-in-the-middle attacks.	Functions solely on third-party integrators to develop security.	Considers edge computing for achieving efficiency.
lxxxii	Qualitative survey and interview-based research on users' privacy perception.	Expresses privacy trade-offs that occur for convenience.	Under-representation of sampling diversity.	Future study to examine trust, risk perception, and awareness towards privacy.
lxxxiii	Assessment of existing privacy for IoT. Experimental study of IoT IP camera	Presents comprehensive analysis of existing protocols. Focusing	Studies the applications of future networks are scant. Highly narrowed	Future works must consider application-based private research for

	privacy threats.	on specific risks in IoT IP camera usage.	scope to IP cameras.	upcoming network technologies. Triggers further research on consumer
lxxxiv	6G survey of threats and possible privacy measures.	Reveals a number of privacy proposals for 6G technology.	Excludes specific 6G applications, such as underwater communications.	Future work: Channel security aspects of connectivity in 6G.
lxxxv	Public Surveillance Privacy Risk Survey.	Discusses in detail how public surveillance affects privacy.	Not covered: network effects of modern networks.	Further study on privacy risk associated with IP cameras and advanced IoT.
lxxxvi	Experimental testing of IoT monitoring devices.	Describes the IoT device monitoring process and privacy	Context for next-generation networks not described.	Recommends further experimentation using modern IoT devices.

		risk involved.		
lxxxvii	Privacy and security consideration of 6G: A review.	In-depth analysis of security for 6G networks.	Little attention toward futuristic network technologies.	Research motivated for integrating AI to deal with security issues.
lxxxviii	AI applications for privacy purposes in the 6G network. Survey of 6G security and privacy technology.	AI's role in solving privacy concerns. Analysis on privacy issues associated with 6G.	Privacy implications are little known. Does not focus on IoT-based security techniques	More research effort needed to explore AI's implications over privacy. Recommends research on authentication protocols for IoT privacy.
lxxxix	Survey of IoT Security Threats within Network	Emphasizes security threats in each layer of IoT	No mention of future networks.	Proposes classification of the threat of 6G network.

	Architecture.	networks.		
xc	Qualitative review of IoT regulations in Australia.	Comprehensive review of Australian regulatory frameworks.	Future-oriented insight is relatively limited.	Recommends extending IoT regulation to fit future needs.
xci	Review of IoT standards and regulations in Australia.	Focuses on the gap in government regulations.	Provides few recommendations for dealing with issues of standards.	Recommends continued monitoring of standards in response to IoT demand.
xcii	Review of security and privacy in 5G and future networks.	Identifies weaknesses due to lack of regulatory standards.	No human-centric security measurements.	Suggests improvement of IoT security for more secure implementations of 5G networks.
xciii	Review of 5G and IoT security issues	Identifies current security challenges for present and future	Focus on regulatory issues and human aspects.	Recommends more research on digital technology challenges.

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

networks.

Strategic Technologies for Securing IoT Networks:

The major areas that have been identified by researchers for emerging networks. These areas include Privacy and Security, which comprise authentication, access control, malicious behavior, encryption, and communications. With the increasing advancements toward futuristic networks, there is a growing interest in a research area for the deployment of modern digital technologies including AI, ML, as well as blockchain on the improvement of security pertaining to these low-powered IoT devices.[xciv] [xcv] [xcvi] [xcvii] This paper will focus on and evaluate these three significant technologies based on their pros and cons and their reliability for improving the security of personal IoT devices in 5G-based networks.

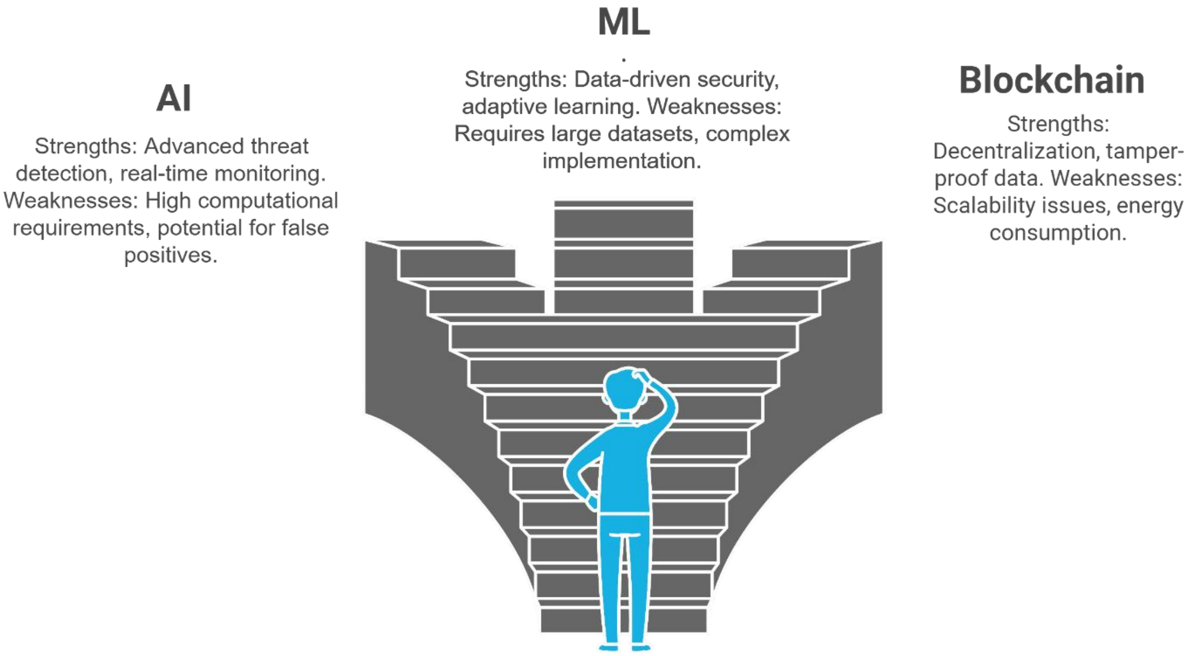
ML
Strengths: Data-driven security, adaptive learning. Weaknesses: Requires large datasets, complex implementation.
AI
Strengths: Advanced threat detection, real-time monitoring. Weaknesses: High computational requirements, potential for false positives.
Blockchain
Strengths: Decentralization, tamper-proof data. Weaknesses: Scalability issues, energy consumption.

Fig 7. Strategic Technologies for Securing IoT Networks

Artificial Intelligence (AI):

In an AI-based IoT system, the decisions will have to be made ahead of an undesirable event that may emerge. It may happen only if there exist robust AI models in IoT. Secondly, a network must consider solving the complication of security within its context to further strengthen it.[xcviii] In all possibilities, there might exist more than one AI-based framework of IoT. There are some important methods and frameworks in all these past searches related to this study.[xcix] [c] [ci] [cii] AI can make things more accurate and run more smoothly. Moreover, it can analyze systems better.[ciii] It has been proved that the large amounts of real-time data from IoT devices help AI systems become more precise.[civ] Integrating the AI and its methods allow IoT technology to grow to its real potential. The technologies within IoT are developed mostly with not-so-great arrangements for security and, hence AI implementation can play major roles while dealing with cyber threats.[cv]

The application of AI in one way or the other, it is definitely the most widely used and applied form of defense and cybersecurity technology. This being the case, 69% of the 850 senior IT executives interviewed told that AI will become efficient even enough to reply to Digital assault in a right way, and 61% believe that AI is going to prove critical when it comes to threat discovery [cvi], [cvii]. All of these stats seem to point in an incredibly strong direction: intense reliance on AI as enhancement addition for cybersecurity. However, the problem in basing the reliance fully on AI as a silver bullet solution to most dilemmas in the cybersecurity context remains inappropriate. Issues at the more integrated and growing positions may negatively affect the work of AI not only to be effective as a device for developing security but for the misuse of cyber-thieves themselves [cviii].

Match, functionality and application put up an entirely different perspective and view when it comes to the true role AI is playing in addressing issues concerning cybersecurity. In essence one of the key benefits of AI is that it works and learns things without all-time monitoring of humans. It would be a programmed machine doing that specific task and performing the relevant checks where it needs a human to do individually [cix]. Simulation of an operation of a neural network, commonly defined as a statistically weighed matrix, makes AI act very close to human decision, giving systematic and rationalized considerations about the options.

It is an only framework of deciding through a neural network and deep learning applied in AI. The nodes within that network are linked functions as the weighted biases at different stages of filtering, assigning the relative values to the diverse rules based on other rules. After the dataset precompiled, it gets saved into any database the given neural network can access. As the system is assimilating prior decisions into information and absorbing new data, it clarifies and develops its understanding about the given task. Based on the absorbed data, artificial intelligence makes biases but with a strategy to create answers according to the analysis of observations. However, that happens in a computerized manner, but the arising biases are part of an algorithm that exists within the design of a model on which ones to include and which to exclude. Therefore, the data to be used here follows all these design requirements and is therefore relevant. However much AI helps in the automation process it has other key characteristics, which in turn add its effectiveness, but also work against its effectiveness.

One key weakness of AI in the field of cybersecurity is its lack of accuracy [cx]. What an AI can do depends on the resources it has. A big neural network, which makes many decisions, requires many processing resources [cxi]. Most of the devices in the IoT cannot execute sophisticated calculations, Hence, AI needs to be pushed further down into the IoT network stack, for example at the edge [cxii]. Despite that, since AI can be given to related systems, such systems also face resource constraints which mean they cannot handle the substantial data demands AI requires. [cxiii].

In response to these capacity constraints, the accuracy of AI needs to be compromised in order to produce systems that are either over-protective in that they would enforce too strong rules or would fail to detect any malicious activity appropriately [cxiv]. If it is overly restrictive, such a system would block rightful usage especially when IoT is associated with a highly automated environment. This could be prevented by relaxing the regulations [cxv] hence leaving entry points to vulnerabilities.

Machine Learning (ML):

Popularly known as machine learning, it has widely been implemented and used in the application of different everyday applications toward the improvement of security and privacy in cyberspace. Algorithms that would predict outcomes with data and statistical analysis would be created, such that the creation of rules will govern its operation. For this reason, it is used like a tool for power over cybercrime. These policies enable ML to make instantaneous decisions for security and privacy augmentation [cxvi]. One of the best examples that are practiced in everyday life using ML is spam email filtering wherein the algorithm is utilized to classify the email address[cxvii]. The context of IoT is quite different from an email. The application of ML to IoT security is basically similar, however. Rules can be defined for creating filters that improve the security of the devices without programming itself [cxviii].

ML is that technique which is applied with AI; it tells computers applying numerous algorithms that enable to learn based on their past experiences without explicit programming of the data. With much less interference of human entities and not so critical mathematical algorithm dynamic networks will be safer due to usage of ML. In very recent periods improvement has gained momentum towards safety in IoTs, it is very much essential these days the machine learning methodologies can hence be used to predict variety of different IoT attacks early on by observing system behavior [cxix]. Such kind of studies have been done in the recent past for edge computing networks [cxx], supply chain [cxxi], UAV networks [cxxii] [cxxiii] and Vehicular networks [cxxiv] [cxxv]to Discuss some areas. For the smart attack detection on IoT devices and a clear strategy to build the defense mechanism, among ML techniques, it comprises of supervised techniques, unsupervised techniques, and reinforcement learning. The most used type of learning. Such supplemented learning has two variations, that is, classifications and regressions. Achieving 5G with AI would be perfect since the IoT key entities like machine learning algorithms are on demand now and would improve healthcare several fold [cxxvi].

While ML is of great value in propelling the state of cybersecurity forward for IoT devices, it does have some significant drawbacks that lessen its ability to function as an effective stand-alone solution to cybercrime. For example, a cyber-criminal could exploit the vulnerabilities of a system through misuse using the help of ML. Through ML, criminals can continue probing a system until it learns its defenses from all these attempts. Such probing insight, eventually, can be useful for a breach to a system. While this may pose some threats, the authors in [cxxvii] argue that ML should be seen as an inevitable part of cybersecurity tools in which enormous advantages exist in protecting the IoT device.

Blockchain:

According to [cxxviii], A blockchain is a decentralized, open-to-all-view database which cannot be easily changed, and hence it is trustable. It uses the network of computers to save data without any central authority. It offers strong ways for verifying identities, managing access to information, and letting users communicate with each other. Further, features such as rule-based agreement, smart contracts, and encryption make it even more secure and reliable. [cxxix]. Blockchain still has some major drawbacks at present that are not applicable in IoT applications on advanced networks. Another very important challenge is the slow processing speed of transactions [cxxx] [cxxxi] [cxxxii]and a lack of scalability [cxxxiii], [cxxxiv], for which solutions are discussed concerning the security concerns below. Research is well in place to cover these areas, though it creates an issue about how blockchain, in its current form, cannot secure IoT data for the coming 5GBN.

Blockchain [cxxxv]can be a vehicle to bring in trust with enhanced security features for the 5G IoT system. It could expedite data exchange while reducing its cost by the introduction of a cryptographic encryption system to the architecture. The immutability and accountability that blockchain can ensure for the system are marvelous [cxxxvi] Blockchain integrated 5G IoT can bring revolution to industrial IoT, Unmanned Autonomous Vehicle (UAV), and so [cxxxvii]. Blockchain and 5G IoT can also be integrated with deep learning.[cxxxviii] The architecture includes the device layer, blockchain network, 5G mobile network, and cloud network [cxxxix]It supports the transmission of data at the speed of 5G through a smart contract. Again, 5G IoT can be integrated with 5G mm-wave technology to design its processing center, object processor, sensing regions and application layer [cxl]These layers use cloud storage and a 5G network to supply services like education, fire station, transportation, factories, etc.

An additional two critical needs for IoT in advanced networks are very-high speed data transfer and extreme scalability. Although it has ensured security, blockchain lags a bit in performance and will still be a challenge if required to be used: As an example, while processing seven transactions per second only, Bitcoin is found feasible [cxli]. Since an RTDPN must produce results in real-time as well, the delayed response time of a block-transaction in blockchain may actually end up being a source of concern. The delay is basically because blockchain is a database; the larger the database, the slower the response times, especially in decentralized networks.[cxlii] [cxliii]Centralized traditional database processes faster because it is managed by a person, organizations, or a group. The control blockchain transfers across the network. This is the reason why the transactions take time [cxliv] [cxlv] [cxlvi] .

Even though it has witnessed such a great number of strides developed in recent research [cxlvii], [cxlviii], and [cxlix] and its well-known advantages as an instrument of cybersecurity, increased adoption made blockchain a prime target for hacking attacks [cl]. Indeed, blockchain technology includes notable security and privacy measures, but blockchain is also susceptible to some threats that undermine data privacy. Some of the most famous is the "51% attack", through which a malicious party becomes in control of more than half of the blockchain ledger, thus allowing this particular party to alter records concerning transactions. Solutions have also been proposed to reduce that risk [cli]. Their effectiveness for IoT devices within a future network, however still waits for further research to become confirmed.

The second is the forking attack, which is an attempt by an attacker to build an alternative chain that competes with the legitimate blockchain. In the event of its success, it might enable fraudulent transactions; however, when it is a "hard fork," the attack becomes irreversible, which is quite dangerous for users of personal IoT devices [clii]. Further concerns are raised in [cliii], where the authors say that a combination of blockchain with those wireless networks sharing the database expose security vulnerabilities to the additive security risks. Such risks include cyberattacks where hackers introduce secret nodes that yield MIM attacks or even spectrum hijacking, showing that after all, blockchain needs to continue evolving further in its security capabilities.

In summary, therefore, while the technologies that constitute contemporary digital discussed can increase security of personal IoT devices in 5G networks, each one has a weakness that presents security threats. As it is noted earlier, such IoT devices usually lack the enough computing power needed to accommodate such technologies, thus this leading to late implementation at the network stack. This therefore leaves the physical layer, on which personal IoT devices will operate, vulnerable to possible exploitation. However, all of the current digital technologies are still important constituents of IoT security. While the research authors of [cliv]and [clv] describe inspirational remedies for the scalability challenge facing blockchain, found within this paper, its proposed implementation is likely impractically constrained. In fact, even more related work, which is described in [clvi]shows that firms have a preference not to utilize proof-of-work-based models more fundamentally for their probabilistic nature and vulnerability towards the possibility of a double-spending attack. Most probably, future blockchain applications for IoT will be consortium blockchains, as described in,[clvii]along with the methods developed by [155] and[154] which further reduce transactional costs and improve network scalabilities so that the whole network is more adapted towards the rapidly expanding market for IoT. Hence, additional research in this domain has to be conducted. As these technologies are further advanced, regulating such devices and ensuring the same ensures safe data communication between these devices will become significant in keeping personal IoT safe. Although modern digital technologies are capable of strengthening the security level of devices, a deficiency in practical and widely applicable standards can weaken the benefit of the technologies if devices themselves are not inherently secure. Summary, therefore, while the technologies that comprise contemporary digital discussed above are capable of enhancing the security of personal IoT devices on 5G networks, each one has a vulnerability that poses a security risk. As already highlighted, the present IoT devices lack computing powers that would be necessary in the deployment of such technologies. Therefore, there's late implementation in the network stack. This therefore makes it leave the physical layer open to exploitation for any IoT devices deployed as personal. Still, all the aforementioned digital technologies remain an integral part of the security of IoTs. Although the research authors of [154]and [154]document inspirational remedies for the scalability challenge faced by blockchain, found within this paper, its proposed implementation is probably impractically constrained. Further related work, in fact, documents in [clviii]shows that firms prefer not to use models based on proof-of-work more fundamentally for their probabilistic nature and susceptibility to the possibility of a double-spending attack. Most probably, the future blockchain applications for IoT will be consortium blockchains, as depicted in [clix]as well as the methods invented by [154]and [154]which also further lower the transaction costs and make the network more scalable in such a way that it can adapt to the quickly growing market of IoT.

As these technologies advance further, regulation of the devices and the requirement to make sure that safe data communication occurs will prove to be of utmost importance for personal IoT devices safety. As much as current digital technologies may enhance security in a device, technology is futile if the very devices on which it is designed to reside are not naturally secure, especially when their lack of standards makes application impractical or impossible on a mass scale.

Significant Outcomes and Future Research

Today's networks, personal IoT devices rely highly on the developers and the users handling personal data collected by the devices. However, since most of the personal IoT devices lack cryptographic functions and because there is a need to reduce energy usage due to minimal power usage, these personal data and other sensitive information such as biometric data are vulnerable to cyber-attacks. The current security paradigm does raise several important questions in the light of the improved battery life and microprocessor performance, for this lack of device-level encryption. Too many devices are easily breached because of a lack of security, and serious breaches await users. Feasibility of physical layer encryption in the light of improvements in battery and microprocessor technology is worth further study.

Technologies like AI, ML, and blockchain have been used to enhance data security. However, though promising, these technologies are found to be ineffective in securing low-power personal IoT devices and, more importantly, cybercriminals have also thrived on their popularity and exploitation. These digital technologies are what low-power IoT devices rely on for security; therefore, any failure in these technologies may expose the devices to cyber threats. The current blockchain is also not suitable for handling high speeds required by 5G networks, which have to process data fast. While research is ongoing to solve these limitations, it requires significant work to be made viable and secure.

These technologies may help cybercriminals seize vulnerabilities of the devices and network, which needs to be defended very strongly.

Current standards are too weak to ensure the confidentiality of IoT data of an individual. With constantly evolving and existing standards, an inconsistency and gap in solutioning IoT security exist. The urgency for an internationally applicable unified set of standards exists for the sake of stronger IoT devices' security on 5G networks. More importantly, standards for personal IoT that involve full security aspects must be established even though IoT standards in electrical and communication safety already exist in the regions of Australia. Even though the security standards were determined collaboratively between Australia and other countries, there should still be uniform minimum standards across the globe to ensure that privacy and security are not compromised based on location.

In summary, the major outcomes of this study are as follows:

- AI for Real-Time Anomaly Detection: AI research using the model, like LSTM has promising power in the real-time detection of anomalies and threats. There is an important need as 5G requires extremely low latency that is absolutely imperative for IoT, and the curbing of cyber threats by the AI-based method of anomaly detection won't let the energy consumption in the IoT devices become excessively high.
- Blockchain for Decentralized Security: the blockchain technology hosts an opportunity for securing decentralized data and offering assurance on privacy as well as integrity without any type of actual centralized authority. With respect to IoT's dream of using almost minimal amounts of energy: security due to decentralization and zero tax on any such device resource.

- According to the research, this will balance well energy efficiency and security of the system. For example, the deployment of lightweight consensus protocols such as PoEW and DAGs in developing better AI models for IoT networks will be key.
- In case of IoT, the primary consideration would be about the energy efficiency since IoT is going to rely on the main low-power devices. As per this paper, AI and blockchain-based security systems are designed to be optimized in a way that will consume minimal power to make security scalable for future applications on 6G networks.
- Conclusion/Future Directions: The paper finally recommends further research to fully develop these technologies for mass deployment in IoT. Further studies on reducing the computational demand of blockchain and AI, security enhancements, and efficiency improvements of 5G infrastructure are recommended in this paper.
- It enlightens the integration of AI and blockchain to provide strong, scalable security for low-power IoT devices in 5G networks. The work on decentralized and energy-efficient solutions is really important as it speaks of the critical need to secure an increasingly vast IoT ecosystem.

Conclusion

This research addresses to the demand of the ever-key security threats that low power IoT devices will face in the 5G network architecture. This is especially due to increasingly connected numbers of IoT devices all over the world with significant ongoing security weaknesses, where most of devices are mounted in the majority of houses and even in critical structures, health systems.

The other considered security framework is blockchain/AI- a combination of strengths from both.AI anomaly detection in real-time and blockchain decentralized integrity of data. This paper discusses major security threats and emerging technologies, which include blockchain, AI in the context of the 5G ecosystem. All reviews are based on strict criteria that have been applied to relevant research studies to serve as the basis on how energy efficiency and scalability can be incorporated into the security solutions designed for IoT networks. Results of the combined effect of AI with blockchain will be there for securing the IoT systems, through optimum balancing between energy efficiency and strong data protection. AI, in real-time, strengthens the process of threat detection, and blockchain offers decentralized data management, thereby eliminating unauthorized access so that integrity of the data is preserved. Still, there arise some problems owing to low computational capability of IoT devices on large-scale deployment. There will be a requirement for more research and development in the architecture of blockchain and AI to reduce computational requirements while scaling up. Besides this, there will be an even greater need for standardizing security protocols all over IoT. This will lead to a necessity of protecting some sensitive data that is applicable application-to-application. Interconnections become more common in life due to IoT as well as 5G. Security solutions entail innovation and energy efficiency to protect user privacy in the network.

References

[i] K. Ashton, ''Internet of Things,'' RFID J., vol. 22, no. 7, pp. 97–114, 2009.

[ii] E. Ahmed, I. Yaqoob, A. Gani, M. Imran, and M. Guizani, ‘‘Internet-ofThings-based smart environments: State of the art, taxonomy, and open research challenges,’’ IEEE Wireless Commun., vol. 23, no. 5, pp. 10–16, Oct. 2016

[iii] L. Atzori, A. Iera, and G. Morabito, ‘‘The Internet of Things: A survey,’’ Comput. Netw., vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[iv] E. Ahmed, I. Yaqoob, A. Gani, M. Imran, and M. Guizani, ‘‘Internet-ofThings-based smart environments: State of the art, taxonomy, and open research challenges,’’ IEEE Wireless Commun., vol. 23, no. 5, pp. 10–16, Oct. 2016. .

[v] Co-Operation With the Working Group RFID of the ETP EPOSS, Internet of Things in 2020, Roadmap for the Future, Version 1.1, INFSO D.4 Networked Enterprise RFID INFSO G.2 Micro Nanosystems, May 2008

[vi] G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. Abu-Mahfouz, ‘‘A survey on 5G networks for the Internet of Things: Communication technologies and challenges,’’ IEEE Access, vol. 6, pp. 3619–3647, 2018.

[vii] S. Li, L. Da Xu, and S. Zhao, ‘‘5G Internet of Things: A survey,’’ J. Ind. Inf. Integr., vol. 10, pp. 1–9, Jun. 2018.

[viii] D. Evans, “The internet of things - how the next evolution of the internet is chaging everything,” White Paper. Cisco Internet Business Solutions Group (IBSG), 2011.

[ix] P. Middleton, P. Kjeldsen, and J. Tully, “Forecast: The internet of things, worldwide, 2013,” Gartner, 2013.

[x] Disruptive Civil Technologies—Six Technologies with Potential Impacts on US Interests Out to 2025-Conference Report CR 2008-07, Nat. Intell. Council, Washington, DC, USA, Apr. 2008.

[xi] I. Yaqoob, E. Ahmed, I. A. T. Hashem, A. I. A. Ahmed, A. Gani, M. Imran, and M. Guizani, ‘‘Internet of Things architecture: Recent advances, taxonomy, requirements, and open challenges,’’ IEEE Wireless Commun., vol. 24, no. 3, pp. 10–16, Jun. 2017.

[xii] Cellular Networks for Massive IoT: Enabling Low Power Wide Area Applications, Ericsson, Stockholm, Sweden, 2016, pp. 1–13

[xiii] Nokia, ‘‘LTE evolution for IoT connectivity,’’ Nokia, Espoo, Finland, White Paper, 2017, pp. 1–18.

[xiv] E. Berthelsen and J. Morrish. (Apr. 2015). ‘‘Forecasting the Internet of Things revenue opportunity.’’ Machina Res., London, U.K., Tech. Rep. [Online]. Available: https://machinaresearch.com/report_pdf/313

[xv] S. Horten, ‘‘Bringing the smart city to life,’’ M2M Alliance J., no. 24, Dec. 2014.

[xvi] S. K. Datta, C. Bonnet, and N. Nikaein, ‘‘An IoT gateway centric architecture to provide novel M2M services,’’ in Proc. IEEE World Forum Internet Things (WF-IoT), Mar. 2014, pp. 514–519.

[xvii]] S. Pellicer, G. Santa, A. L. Bleda, R. Maestre, A. J. Jara, and A. G. Skarmeta, ‘‘A global perspective of smart cities: A survey,’’ in Proc. IEEE 7th Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput. (IMIS), Jul. 2013, pp. 439–444.

[xviii]] Z. M. Fadlullah, M. M. Fouda, N. Kato, A. Takeuchi, N. Iwasaki, and Y. Nozaki, ‘‘Toward intelligent machine-to-machine communications in smart grid,’’ IEEE Commun. Mag., vol. 49, no. 4, pp. 60–65, Apr. 2011

[xix] B. Silva, R. M. Fisher, A. Kumar, and G. P. Hancke, ‘‘Experimental link quality characterization of wireless sensor networks for underground monitoring,’’ IEEE Trans. Ind. Informat., vol. 11, no. 5, pp. 1099–1110, Oct. 2015.

[xx] A. M. Abu-Mahfouz, Y. Hamam, P. R. Page, K. Djouani, and A. Kurien, ‘‘Real-time dynamic hydraulic model for potable water loss reduction,’’ Procedia Eng., vol. 154, no. 8, pp. 99–106, 2016.

[xxi]M. Agiwal, A. Roy, and N. Saxena, "Next Generation 5G Wireless Networks: A Comprehensive Survey," IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 1617–1655, 2016.

[xxii] P. Zhang, X. Yang, J. Chen, and Y. Huang, "A Survey of Testing for 5G: Solutions, Opportunities, and Challenges," China Communications, vol. 16, no. 1, pp. 69–85, 2019.

[xxiii] M. Liyanage, I. Ahmad, A. B. Abro, A. Gurtov, and M. Ylianttila, A Comprehensive Guide to 5G Security. Wiley Publishing, 2018.

[xxiv] S. Zhang, "An Overview of Network Slicing for 5G," IEEE Wireless Communications, 2019.

[xxv] M. S. Bonfim, K. L. Dias, and S. F. Fernandes, "Integrated NFV/SDN Architectures: A Systematic Literature Review," ACM Computing Surveys (CSUR), vol. 51, no. 6, p. 114, 2019.

[xxvi] R. N. Mitra and D. P. Agrawal, "5G Mobile Technology: A Survey," ICT Express, vol. 1, no. 3, pp. 132–137, 2015.

[xxvii] S. E. Elayoubi, M. Fallgren, P. Spapis, G. Zimmermann, D. Mart´ınSacristan, C. Yang, S. Jeux, P. Agyapong, L. Campoy, Y. Qi ´ et al., "5G Service Requirements and Operational Use Cases: Analysis and METIS II Vision," in Networks and Communications (EuCNC), 2016 European Conference on. IEEE, 2016, pp. 158–162.

[xxviii] P. Lapsley, "The History of Phone Phreaking," Exploding the Phone, pp. 2005–2009, 2011.

[xxix] S. Gold, "The Rebirth of Phreaking," Network security, vol. 2011, no. 6, pp. 15–17, 2011.

[xxx] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues,"

IEEE Communications Surveys & Tutorials, vol. 17, no. 3, pp. 1294–1312, 2015.

[xxxi]] A. Rayes and S. Salam, ‘‘Internet of Things (IoT) overview,’’ in Internet of Things From Hype to Reality. Springer, Oct. 2016, pp. 1–34.

[xxxii] W. Yimyam, K. Kocento, and M. Ketcham, ‘‘Video surveillance system using IP camera for target person detection,’’ in Proc. 18th Int. Symp. Commun. Inf. Technol. (ISCIT), Sep. 2018, pp. 176–179.

[xxxiii] B. Matthews, D. Nielsen, J. Schade, K. Chan, and M. Kiniry, ‘‘Automated discovery of flight track anomalies,’’ in Proc. 33rd Digital Avionics Syst. Conf. (DASC), 2014, pp. 1–15.

[xxxiv] C. Lutz and G. Newlands, ‘‘Privacy and smart speakers: A multidimensional approach,’’ Inf. Soc., vol. 37, no. 3, pp. 147–162, Mar. 2021

[xxxv] J. Streiff, O. Kenny, S. Das, A. Leeth, and L. J. Camp, ‘‘Who’s watching your child? Exploring home security risks with smart toy bears,’’ in Proc. IEEE/ACM 3rd Int. Conf. Internet-of-Things Design Implement. (IoTDI), Jun. 2018, pp. 285–286

[xxxvi] C. Lutz and G. Newlands, ‘‘Privacy and smart speakers: A multidimensional approach,’’ Inf. Soc., vol. 37, no. 3, pp. 147–162, Mar. 2021.

[xxxvii] J. Streiff, O. Kenny, S. Das, A. Leeth, and L. J. Camp, ‘‘Who’s watching your child? Exploring home security risks with smart toy bears,’’ in Proc. IEEE/ACM 3rd Int. Conf. Internet-of-Things Design Implement. (IoTDI), Jun. 2018, pp. 285–286.

J. Streiff, O. Kenny, S. Das, A. Leeth, and L. J. Camp, ‘‘Who’s watching your child? Exploring home security risks with smart toy bears,’’ in Proc. IEEE/ACM 3rd Int. Conf. Internet-of-Things Design Implement. (IoTDI), Jun. 2018, pp. 285–286.

[xxxix] Y. Jia, Y. Xiao, J. Yu, X. Cheng, Z. Liang, and Z. Wan, ‘‘A novel graphbased mechanism for identifying traffic vulnerabilities in smart home IoT,’’ in Proc. IEEE INFOCOM - IEEE Conf. Comput. Commun., Apr. 2018, pp. 1493–1501.

[xl]] S. Godwin, B. Glendenning, and K. Gagneja, ‘‘Future security of smart speaker and IoT smart home devices,’’ in Proc. 5th Conf. Mobile Secure Services (MobiSecServ), Mar. 2019, pp. 1–6.

[xli] A. Yazdinejad, A. Dehghantanha, R. M. Parizi, G. Srivastava, and H. Karimipour, “Secure intelligent fuzzy blockchain framework: Effective threat detection in iot networks,” Computers in Industry, vol. 144, p. 103801, 2023

[xlii] D. B. Unsal, T. S. Ustun, S. M. S. Hussain, and A. Onen, ‘‘Enhancing cybersecurity in smart grids: False data injection and its mitigation,’’ Energies, vol. 14, no. 9, p. 2657, May 2021.

[xliii] Z. He, T. Miari, H. M. Makrani, M. Aliasgari, H. Homayoun, and H. Sayadi, ‘‘When machine learning meets hardware cybersecurity: Delving into accurate zero-day malware detection,’’ in Proc. 22nd Int. Symp. Quality Electron. Design (ISQED), May 2021, pp. 85–90.

[xliv] A. Bourechak, O. Zedadra, M. N. Kouahla, A. Guerrieri, H. Seridi, and G. Fortino, ‘‘At the confluence of artificial intelligence and edge computing in IoT-based applications: A review and new perspectives,’’ Sensors, vol. 23, no. 3, p. 1639, Feb. 2023

[xlv] M. Brundage, ‘‘The malicious use of artificial intelligence: Forecasting, prevention, and mitigation,’’ 2018, arXiv:1802.07228.

[xlvi] M. Wazid, A. K. Das, V. Chamola, and Y. Park, ‘‘Uniting cyber security and machine learning: Advantages, challenges and future research,’’ ICT Exp., vol. 8, no. 3, pp. 313–321, Sep. 2022.

[xlvii] T. M. Mitchell, ‘‘Does machine learning really work?’’ AI Mag., vol. 18, no. 3, p. 11, Sep. 1997.

[xlviii] E. G. Dada, J. S. Bassi, H. Chiroma, S. M. Abdulhamid, A. O. Adetunmbi, and O. E. Ajibuwa, ''Machine learning for email spam filtering: Review, approaches and open research problems,'' Heliyon, vol. 5, no. 6, Jun. 2019, Art. no. e01802.

[xlix] R. Tolido. (2019). Reinventing Cybersecurity With Artificial Intelligence. [Online]. Accessed: Sep. 29, 2022. [Online]. Available: https://www.capgemini.com/au-en/wp-content/uploads/ sites/9/2019/07/AI-in-Cybersecurity_Report_20190711_V06.pdf

[l] L. Lazić, ''Benefit from AI in cybersecurity,'' in Proc. 11th Int. Conf. Bus. Inf. Secur. (BISEC), Jan. 2019, pp. 103–119

[li] J.-H. Li, ''Cyber security meets artificial intelligence: A survey,'' Frontiers Inf. Technol. Electron. Eng., vol. 19, no. 12, pp. 1462–1474, Dec. 2018.

[lii] J.-H. Li, ''Cyber security meets artificial intelligence: A survey,'' Frontiers Inf. Technol. Electron. Eng., vol. 19, no. 12, pp. 1462–1474, Dec. 2018.

[liii] M. I. Baba, N. Nafees, I. Manzoor, K. A. Naik, and S. Ahmed, "Evolution of Mobile Wireless Communication Systems from 1G to 5G: A Comparative Analysis," 2018.

[liv] P. Lapsley, "The History of Phone Phreaking," Exploding the Phone, pp. 2005–2009, 2011.

[lv] C. Hanser, S. Moritz, F. Zaloshnja, and Q. Zhang, "Security in Mobile Telephony: The Security Levels in the Different Handy Generations," Uppsala Universitet, Uppsala, 2014.

[lvi] Y. E. H. El Idrissi, N. Zahid, and M. Jedra, "Security Analysis of 3GPP (LTE)WLAN Interworking and a New local Authentication Method Based on EAP-AKA," in The First International Conference on Future Generation Communication Technologies. IEEE, 2012, pp. 137–142.

[lvii] M. Liyanage and A. Gurtov, “Secured VPN Models for LTE Backhaul Networks,” in 2012 IEEE Vehicular Technology Conference (VTC Fall). IEEE, 2012, pp. 1–5.

[lviii] C. Hanser, S. Moritz, F. Zaloshnja, and Q. Zhang, “Security in Mobile Telephony: The Security Levels in the Different Handy Generations,” Uppsala Universitet, Uppsala, 2014.

[lix] M. Liyanage, M. Ylianttila, and A. Gurtov, “A Case Study on Security Issues in LTE Backhaul and Core Networks,” Case Studies in Secure Computing: Achievements and Trends, vol. 1, p. 167, 2014.

[lx] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, “Security for 4G and 5G Cellular networks: A Survey of Existing Authentication and Privacy-Preserving Schemes,” Journal of Network and Computer Applications, vol. 101, pp. 55–82, 2018.

[lxi] S. K. Mohapatra, B. R. Swain, and P. Das, “Comprehensive Survey of Possible Security Issues on 4G Networks,” International Journal of Network Security & Its Applications, vol. 7, no. 2, p. 61, 2015.

[lxii] S. K. Mohapatra, B. R. Swain, and P. Das, “Comprehensive Survey of Possible Security Issues on 4G Networks,” International Journal of Network Security & Its Applications, vol. 7, no. 2, p. 61, 2015.

[lxiii] B. Kitchenham, S. Charters et al., “Guidelines for performing systematic literature reviews in software engineering version 2.3,” Engineering, vol. 45, no. 4ve, p. 1051, 2007.

[lxiv] P. V. Torres-Carrion, C. S. Gonz ´ alez-Gonz ´ alez, S. Aciar, and ´ G. Rodr´ıguez-Morales, “Methodology for systematic literature review applied to engineering and education,” in 2018 IEEE Global engineering education conference (EDUCON). IEEE, 2018, pp. 1364–1373

[lxv] Q. Tang, O. Ermis, C. D. Nguyen, A. De Oliveira, and A. Hirtzig, "A systematic analysis of 5g networks with a focus on 5g core security," IEEE Access, vol. 10, pp. 18 298–18 319, 2022.

[lxvi] M. Liyanage, I. Ahmad, A. B. Abro, A. Gurtov, and M. Ylianttila, A comprehensive guide to 5G security. Wiley Online Library, 2018.

[lxvii] B. Kitchenham, S. Charters et al., "Guidelines for performing systematic literature reviews in software engineering version 2.3," Engineering, vol. 45, no. 4ve, p. 1051, 2007

[lxviii] A. Dutta and E. Hammad, "5g security challenges and opportunities: a system approach," in 2020 IEEE 3rd 5G World Forum (5GWF). IEEE, 2020, pp. 109–114.

[lxix] P. Porambage, G. Gür, D. P. Moya Osorio, M. Livanage, and M. Ylianttila, ''6G security challenges and potential solutions,'' in Proc. Joint Eur. Conf. Netw. Commun. 6G Summit (EuCNC/6G Summit), Jun. 2021, pp. 622–627.

[lxx] M. Wang, T. Zhu, T. Zhang, J. Zhang, S. Yu, and W. Zhou, ''Security and privacy in 6G networks: New areas and new challenges,'' Digit. Commun. Netw., vol. 6, no. 3, pp. 281–291, Aug. 2020.

[lxxi] V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang, and Y.-D. Lin, ''Security and privacy for 6G: A survey on prospective technologies and challenges,'' IEEE Commun. Surveys Tuts., vol. 23, no. 4, pp. 2384–2428, 4th Quart., 2021.

[lxxii] M. Wang, T. Zhu, T. Zhang, J. Zhang, S. Yu, and W. Zhou, ''Security and privacy in 6G networks: New areas and new challenges,'' Digit. Commun. Netw., vol. 6, no. 3, pp. 281–291, Aug. 2020.

[lxxiii] . Hung, D. Liau, S.-Y. Lien, and K.-C. Chen, ''Low latency communication for Internet of Things,'' in Proc. IEEE/CIC Int. Conf. Commun. China (ICCC), Nov. 2015, pp. 1–6.

[lxxiv]] S. Ahmadzadeh, G. Parr, and W. Zhao, ‘‘A review on communication aspects of demand response management for future 5G IoT-based smart grids,’’ IEEE Access, vol. 9, pp. 77555–77571, 2021.

[lxxv]] L. Mostarda, A. Navarra, and F. Nobili, ‘‘Fast file transfers from IoT devices by using multiple interfaces,’’ Sensors, vol. 21, no. 1, p. 36, Dec. 2020.

[lxxvi] M. Siddiqi, H. Yu, and J. Joung, ‘‘5G ultra-reliable low-latency communication implementation challenges and operational issues with IoT devices,’’ Electronics, vol. 8, no. 9, p. 981, Sep. 2019..

[lxxvii] S. Sicari, A. Rizzardi, and A. Coen-Porisini, ‘‘5G in the Internet of Things era: An overview on security and privacy challenges,’’ Comput. Netw., vol. 179, Oct. 2020, Art. no. 107345.

[lxxviii]L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, ‘‘IoT privacy and security: Challenges and solutions,’’ Appl. Sci., vol. 10, no. 12, p. 4102, Jun. 2020.

[lxxix] N. Panwar, S. Sharma, and A. K. Singh, “A Survey on 5G: The Next Generation of Mobile Communication,” Physical Communication, vol. 18, pp. 64–84, 2016.

[lxxx] D. Rupprecht, A. Dabrowski, T. Holz, E. Weippl, and C. Popper, “On ¨ Security Research towards Future Mobile Network Generations,” IEEE Communications Surveys & Tutorials, 2018.

[lxxxi] J. C.-W. Lin, G. Srivastava, Y. Zhang, Y. Djenouri, and M. Aloqaily, ‘‘Privacy-preserving multiobjective sanitization model in 6G IoT environments,’’ IEEE Internet Things J., vol. 8, no. 7, pp. 5340–5349, Apr. 2021

[lxxxii] I. Psychoula, D. Singh, L. Chen, F. Chen, A. Holzinger, and H. Ning, ‘‘Users’ privacy concerns in IoT based applications,’’ in Proc.

IEEE SmartWorld, Ubiquitous Intell. Comput., Adv. Trusted Comput., Scalable Comput. Commun., Cloud Big Data Comput., Internet People Smart City Innov. (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), Oct. 2018, pp. 1887–1894

[lxxxiii] M. Seliem, K. Elgazzar, and K. Khalil, ‘‘Towards privacy preserving IoT environments: A survey,’’ Wireless Commun. Mobile Comput., vol. 2018, pp. 1–15, Nov. 2018.

[lxxxiv] A. L. Imoize, O. Adedeji, N. Tandiya, and S. Shetty, ‘‘6G enabled smart infrastructure for sustainable society: Opportunities, challenges, and research roadmap,’’ Sensors, vol. 21, no. 5, p. 1709, Mar. 2021.

[lxxxv] S. Moncrieff, S. Venkatesh, and G. A. W. West, ‘‘Dynamic privacy in public surveillance,’’ Computer, vol. 42, no. 9, pp. 22–28, Sep. 2009.

[lxxxvi] V. Sivaraman, H. Gharakheili, C. Fernandes, N. Clark, and T. Karliychuk, ‘‘Smart IoT devices in the home: Security and privacy implications,’’ IEEE Technol. Soc. Mag., vol. 37, no. 2, pp. 71–79, Jun. 2018.

[lxxxvii] M. Wang, T. Zhu, T. Zhang, J. Zhang, S. Yu, and W. Zhou, ‘‘Security and privacy in 6G networks: New areas and new challenges,’’ Digit. Commun. Netw., vol. 6, no. 3, pp. 281–291, Aug. 2020.

[lxxxviii] Y. Siriwardhana, P. Porambage, M. Liyanage, and M. Ylianttila, ‘‘AI and 6G security: Opportunities and challenges,’’ in Proc. Joint Eur. Conf. Netw. Commun. 6G Summit (EuCNC/6G Summit), Jun. 2021, pp. 616–621.

[lxxxix] H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai, ''A survey of IoT security based on a layered architecture of sensing and data analysis,'' Sensors, vol. 20, no. 13, p. 3625, Jun. 2020.

[xc] Harkin, M. Mann, and I. Warren, ''Consumer IoT and its underregulation: Findings from an Australian study,'' Policy Internet, vol. 14, no. 1, pp. 96–113, Feb. 2022.

[xci] Internet of Things in Communications Occasional Paper. Accessed: Aug. 28, 2022. [Online]. Available: https://www.acma.gov.au/sites/ default/files/2020-07/Internet%20of%20Things%20in%20media%20and %20communications_Occasional%20paper.pdf

[xcii] F. Salahdine, T. Han, and N. Zhang, ''Security in 5G and beyond recent advances and future challenges,'' Secur. Privacy, vol. 6, no. 1, p. e271, Jan. 2023

[xciii] G. E. P. Kumar, M. Lydia, and Y. Levron, ''Security challenges in 5G and IoT networks: A review,'' in Secure Communication for 5G and IoT Networks. 2022, pp. 1–13.

[xciv] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K.-K.-R. Choo, ''A systematic literature review of blockchain cyber security,'' Digit. Commun. Netw., vol. 6, no. 2, pp. 147–156, May 2020.

[xcv] B. Alotaibi, ''Utilizing blockchain to overcome cyber security concerns in the Internet of Things: A review,'' IEEE Sensors J., vol. 19, no. 23, pp. 10953–10971, Dec. 2019.

[xcvi] C. Ma, ''Smart city and cyber-security; technologies used, leading challenges and future recommendations,'' Energy Rep., vol. 7, pp. 7999–8012, Nov. 2021.

[xcvii]] B. S. Sagar, S. Niranjan, N. Kashyap, and D. N. Sachin, ''Providing cyber security using artificial intelligence—A survey,'' in

Proc. 3rd Int. Conf. Comput. Methodologies Commun. (ICCMC), Mar. 2019, pp. 717–720.

[xcviii] Mohanta BK, Jena D, Satapathy U, Patnaik S. Survey on IoT security: challenges and solution using machine learning, artificial intelligence and blockchain technology. *Internet of Things*. 2020; **11**:100227.

[xcix] Kotenko I, Saenko I, Branitskiy A. Framework for mobile Internet of Things security monitoring based on big data processing and machine learning. *IEEE Access*. 2018;

[c] Hossain E, Khan I, Un-Noor F, Sikander SS, Sunny MSH. Application of big data and machine learning in smart grid, and associated security concerns: a review. *IEEE Access*. 2019;

[ci] Chaabouni N, Mosbah M, Zemmari A, Sauvignac C, Faruki P. Network intrusion detection for IoT security based on learning techniques. *IEEE Commun Surv Tutor*. 2019;

[cii] Anthi E, Williams L, Słowińska M, Theodorakopoulos G, Burnap P. A supervised intrusion detection system for smart home IoT devices. *IEEE Internet Things J*. 2019;

[ciii] Mohanta BK, Jena D, Satapathy U, Patnaik S. Survey on IoT security: challenges and solution using machine learning, artificial intelligence and blockchain technology. *Internet of Things*. 2020;

[civ] Ghosh A, Chakraborty D, Law A. Artificial intelligence in Internet of Things. *CAAI Trans Intell Technol*. 2018; **3**(4): 208-218.

[cv] Wang S, Qiao Z. Robust pervasive detection for adversarial samples of artificial intelligence in IoT environments. *IEEE Access*. 2019;

[cvi] R. Tolido. (2019). Reinventing Cybersecurity With Artificial Intelligence. [Online]. Accessed: Sep. 29, 2022. [Online]. Available:

https://www.capgemini.com/au-en/wp-content/uploads/sites/9/2019/07/AI-in-Cybersecurity_Report_20190711_V06.pdf

[cvii] L. Lazić, ‘‘Benefit from AI in cybersecurity,’’ in Proc. 11th Int. Conf. Bus. Inf. Secur. (BISEC), Jan. 2019, pp. 103–119.

[cviii] M. Brundage, ‘‘The malicious use of artificial intelligence: Forecasting, prevention, and mitigation,’’ 2018, arXiv:1802.07228.

[cix] J.-H. Li, ‘‘Cyber security meets artificial intelligence: A survey,’’ Frontiers Inf. Technol. Electron. Eng., vol. 19, no. 12, pp. 1462–1474, Dec. 2018.

[cx] J. Kim and N. Park, ‘‘Blockchain-based data-preserving AI learning environment model for AI cybersecurity systems in IoT service environments,’’ Appl. Sci., vol. 10, no. 14, p. 4718, Jul. 2020.

[cxi] S. Zhao, S. Li, L. Qi, and L. D. Xu, ‘‘Computational intelligence enabled cybersecurity for the Internet of Things,’’ IEEE Trans. Emerg. Topics Comput. Intell., vol. 4, no. 5, pp. 666–674, Oct. 2020.

[cxii] A. Bourechak, O. Zedadra, M. N. Kouahla, A. Guerrieri, H. Seridi, and G. Fortino, ‘‘At the confluence of artificial intelligence and edge computing in IoT-based applications: A review and new perspectives,’’ Sensors, vol. 23, no. 3, p. 1639, Feb. 2023.

[cxiii] Z. Zhang, H. Ning, F. Shi, F. Farha, Y. Xu, J. Xu, F. Zhang, and K.-K.-R. Choo, ‘‘Artificial intelligence in cyber security: Research advances, challenges, and opportunities,’’ Artif. Intell. Rev., vol. 55, no. 2, pp. 1029–1053, Mar. 2021.

[cxiv] Z. Zhang, H. Ning, F. Shi, F. Farha, Y. Xu, J. Xu, F. Zhang, and K.-K.-R. Choo, ‘‘Artificial intelligence in cyber security: Research advances, challenges, and opportunities,’’ Artif. Intell. Rev., vol. 55, no. 2, pp. 1029–1053, Mar. 2021.

[cxv] T. C. Truong, I. Zelinka, J. Plucar, M. Čandík, and V. Šulc, ‘‘Artificial intelligence and cybersecurity: Past, presence, and future,’’ in

Artificial Intelligence and Evolutionary Computations in Engineering Systems. Singapore: Springer, 2020, pp. 351–363

[cxvi] T. M. Mitchell, ‘‘Does machine learning really work?’’ AI Mag., vol. 18, no. 3, p. 11, Sep. 1997.

[cxvii] E. G. Dada, J. S. Bassi, H. Chiroma, S. M. Abdulhamid, A. O. Adetunmbi, and O. E. Ajibuwa, ‘‘Machine learning for email spam filtering: Review, approaches and open research problems,’’ Heliyon, vol. 5, no. 6, Jun. 2019, Art. no. e01802.

[cxviii] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, ‘‘Machine learning in IoT security: Current solutions and future challenges,’’ IEEE Commun. Surveys Tuts., vol. 22, no. 3, pp. 1686–1721, 3rd Quart., 2020.

[cxix] V. Chamola, V. Hassija, S. Gupta, A. Goyal, M. Guizani, and B. Sikdar, "Disaster and pandemic management using machine learning: a survey," IEEE Internet of Things Journal, 2020.

[cxx] S. Singh, R. Sulthana, T. Shewale, V. Chamola, A. Benslimane, and B. Sikdar, "Machine learning assisted security and privacy provisioning for edge computing: A survey," IEEE Internet of Things Journal, 2021.

[cxxi] T. Alladi, V. Chamola, B. Sikdar, and K.-K. R. Choo, "Consumer iot: Security vulnerability case studies and solutions," IEEE Consumer Electronics Magazine, vol. 9, no. 2, pp. 17–25, 2020.

[cxxii] V. Hassija, V. Chamola, A. Agrawal, A. Goyal, N. C. Luong, D. Niyato, F. R. Yu, and M. Guizani, "Fast, reliable, and secure drone communication: A comprehensive survey," arXiv preprint arXiv:2105.01347, 2021.

[cxxiii] V. Chamola, P. Kotesh, A. Agarwal, N. Gupta, M. Guizani et al., "A comprehensive review of unmanned aerial vehicle attacks and neutralization techniques," Ad Hoc Networks, p. 102324, 2020

[cxxiv] T. Alladi, V. Kohli, V. Chamola, F. R. Yu, and M. Guizani, “Artificial intelligence (ai)-empowered intrusion detection architecture for the internet of vehicles,” IEEE Wireless Communications, vol. 28, no. 3, pp. 144–149, 2021.

[cxxv] H. Grover, T. Alladi, V. Chamola, D. Singh, and K.-K. R. Choo, “Edge computing and deep learning enabled secure multi-tier network for internet of vehicles,” IEEE Internet of Things Journal, pp. 1–1, 2021.

[cxxvi] H. K. Bharadwaj, A. Agarwal, V. Chamola, N. R. Lakkaniga, V. Hassija, M. Guizani, and B. Sikdar, “A review on the role of machine learning in enabling iot based healthcare applications,” IEEE Access, vol. 9, pp. 38 859–38 890, 2021.

[cxxvii] M. Wazid, A. K. Das, V. Chamola, and Y. Park, ‘‘Uniting cyber security and machine learning: Advantages, challenges and future research,’’ ICT Exp., vol. 8, no. 3, pp. 313–321, Sep. 2022

[cxxviii] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, D. Niyato, O. Dobre, and H. V. Poor, ‘‘6G Internet of Things: A comprehensive survey,’’ IEEE Internet Things J., vol. 9, no. 1, pp. 359–383, Jan. 2021

[cxxix] M. Wang, T. Zhu, T. Zhang, J. Zhang, S. Yu, and W. Zhou, ‘‘Security and privacy in 6G networks: New areas and new challenges,’’ Digit. Commun. Netw., vol. 6, no. 3, pp. 281–291, Aug. 2020

[cxxx] I. A. Omar, R. Jayaraman, K. Salah, I. Yaqoob, and S. Ellahham, ‘‘Applications of blockchain technology in clinical trials: Review and open challenges,’’ Arabian J. Sci. Eng., vol. 46, no. 4, pp. 3001–3015, Oct. 2020.

[cxxxi] V. Patel, F. Khatiwala, K. Shah, and Y. Choksi, ‘‘A review on blockchain technology: Components, issues and challenges,’’ in

ICDSMLA (Lecture Notes in Electrical Engineering). Singapore: Springer, 2020, pp. 1257–1262.

[cxxxii] V. L. Lemieux, ''Trusting records: Is blockchain technology the answer?'' Records Manage. J., vol. 26, no. 2, pp. 110–139, Jul. 2016.

[cxxxiii] M. J. M. Chowdhury, A. Colman, M. A. Kabir, J. Han, and P. Sarda, ''Blockchain versus database: A critical analysis,'' in Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE), Aug. 2018, pp. 1348–1353

[cxxxiv] D. Khan, L. T. Jung, and M. A. Hashmani, ''Systematic literature review of challenges in blockchain scalability,'' Appl. Sci., vol. 11, no. 20, p. 9372, Oct. 2021.

[cxxxv] Haque AKMB, Bhushan B, Hasan M, Zihad MM (2022) Revolutionizing the industrial internet of things using blockchain: an unified approach. In: Balas VE, Solanki VK, Kumar R (eds) Recent advances in internet of things and machine learning. Intelligent systems reference library, vol 215. Springer, Cham. https://doi.org/10.1007/978-3-030-90119-6_5

[cxxxvi] Hewa TM, Kalla A, Nag A, Ylianttila ME, Liyanage M (2020) Blockchain for 5G and IoT: opportunities and challenges. In: IEEE eighth international conference on communications and networking (ComNet), pp 1–8. https://doi.org/10.1109/ComNet47917.2020.9306082

[cxxxvii] Haque AKMB, Shurid S, Juha AT, Sadique MS, Asaduzzaman AS (2020) A novel design of gesture and voice controlled solar-powered smart wheel chair with obstacle detection. In: 2020 IEEE international conference on informatics, IoT, and enabling technologies (ICIoT). https://doi.org/ 10.1109/iciot48696.2020.9089652

[cxxxviii] Kaur UK, Shalu (2021) Deep learning approach for resource optimization in blockchain, cellular networks, and IoT: open challenges and current solutions. https://doi.org/10.1002/978111978 5873.ch16

[cxxxix] Satpathy S, Mahapatra S, Singh A (2021) Fusion of blockchain technology with 5G: a symmetric beginning. In: Tanwar S (eds) Blockchain for 5G-enabled IoT. Springer, Cham. https://doi.org/ 10.1007/978-3-030-67490-8_3

[cxl] Haque AK, Bhushan B (2021c) Blockchain in a nutshell. Adv Data Min Database Manage 124–143. https://doi.org/10.4018/978-1-7998-6694-7.ch009

[cxli] A. Chauhan, O. P. Malviya, M. Verma, and T. S. Mor, ''Blockchain and scalability,'' in Proc. IEEE Int. Conf. Softw. Qual., Rel. Secur. Companion (QRS-C), Jun. 2018, pp. 122–128

[cxlii] P. Tasatanattakool and C. Techapanupreeda, ''Blockchain: Challenges and applications,'' in Proc. Int. Conf. Inf. Netw. (ICOIN), 2018, pp. 473–475.

[cxliii] D. Fisher, ''Incremental, approximate database queries and uncertainty for exploratory visualization,'' in Proc. IEEE Symp. Large Data Anal. Visualizat., Oct. 2011, pp. 73–80

[cxliv] S. Arif, M. A. Khan, S. Rehman, M. A. Kabir, and M. Imran, ''Investigating smart home security: Is blockchain the answer?'' IEEE Access, vol. 8, pp. 117802–117816, 2020.

[cxlv] J. Newell, Q. Mamun, S. Rehman, and M. Z. Islam, ''Proof-ofenough-work consensus algorithm for enhanced transaction processing in blockchain,'' in Proc. IEEE Wireless Commun. Netw. Conf. (WCNC), Apr. 2022, pp. 1188–1193

[cxlvi] B. Shabandri and P. Maheshwari, ''Enhancing IoT security and privacy using distributed ledgers with IOTA and the tangle,'' in Proc.

6th Int. Conf. Signal Process. Integr. Netw. (SPIN), Mar. 2019, pp. 1069–1075.

[cxlvii] S. Arif, M. A. Khan, S. Rehman, M. A. Kabir, and M. Imran, ''Investigating smart home security: Is blockchain the answer?'' IEEE Access, vol. 8, pp. 117802–117816, 2020.

[cxlviii] J. Newell, Q. Mamun, S. Rehman, and M. Z. Islam, ''Proof-ofenough-work consensus algorithm for enhanced transaction processing in blockchain,'' in Proc. IEEE Wireless Commun. Netw. Conf. (WCNC), Apr. 2022, pp. 1188–1193.

[cxlix] B. Shabandri and P. Maheshwari, ''Enhancing IoT security and privacy using distributed ledgers with IOTA and the tangle,'' in Proc. 6th Int. Conf. Signal Process. Integr. Netw. (SPIN), Mar. 2019, pp. 1069–1075.

[cl] . Wang, C. Wang, and Q. Hu, ''Corking by forking: Vulnerability analysis of blockchain,'' in Proc. IEEE INFOCOM Conf. Comput. Commun., Apr. 2019, pp. 829–837

[cli] C. Ye, G. Li, H. Cai, Y. Gu, and A. Fukuda, ''Analysis of security in blockchain: Case study in 51%-attack detecting,'' in Proc. 5th Int. Conf

[clii] . Ramos, F. Pianese, T. Leach, and E. Oliveras, ''A great disturbance in the crypto: Understanding cryptocurrency returns under attacks,'' Blockchain, Res. Appl., vol. 2, no. 3, Sep. 2021, Art. no. 100021.

[cliii] K. Ramezanpour, J. Jagannath, and A. Jagannath, ''Security and privacy vulnerabilities of 5G/6G and WiFi 6: Survey and research directions from a coexistence perspective,'' Comput. Netw., vol. 221, Feb. 2023, Art. no. 109515

[cliv] J. Newell, Q. Mamun, S. Rehman, and M. Z. Islam, ''Proof-ofenough-work consensus algorithm for enhanced transaction

processing in blockchain,'' in Proc. IEEE Wireless Commun. Netw. Conf. (WCNC), Apr. 2022, pp. 1188–1193.

[clv] B. Shabandri and P. Maheshwari, ''Enhancing IoT security and privacy using distributed ledgers with IOTA and the tangle,'' in Proc. 6th Int. Conf. Signal Process. Integr. Netw. (SPIN), Mar. 2019, pp. 1069–1075.

[clvi] R. Han, V. Gramoli, and X. Xu, ''Evaluating blockchains for IoT,'' in Proc. 9th IFIP Int. Conf. New Technol., Mobility Secur. (NTMS), Feb. 2018, pp. 1–5.

[clvii] . Arif, M. A. Khan, S. Rehman, M. A. Kabir, and M. Imran, ''Investigating smart home security: Is blockchain the answer?'' IEEE Access, vol. 8, pp. 117802–117816, 2020

[clviii] R. Han, V. Gramoli, and X. Xu, ''Evaluating blockchains for IoT,'' in Proc. 9th IFIP Int. Conf. New Technol., Mobility Secur. (NTMS), Feb. 2018, pp. 1–5.

[clix] . Arif, M. A. Khan, S. Rehman, M. A. Kabir, and M. Imran, ''Investigating smart home security: Is blockchain the answer?'' IEEE Access, vol. 8, pp. 117802–117816, 2020