Mesopotamian journal of Cybersecurity
Vol.5,No.1, **pp**. 187–201
DOI: https://doi.org/10.58496/MJCS/2025/013; ISSN: 2958-6542
https://mesopotamian.press/journals/index.php/cybersecurity

Research Article

Internet of Things for Smart Building Security: Leveraging a Blockchain for Enhanced IoT Security

Adnane AL KARKOURI [1,*], Zahra Oughannou[2], Oussama El Gannour[3,4], Toufik Mzili [5], Salmane Bourekkadi [6,1]

[1] *Ibn Tofail University, Kenitra, Morocco.*

[2] *Innovation in Mathematics and Intelligent Systems (IMIS) Laboratory, Ibn Zohr University, Agadir, Morocco.*

[3] *LIASSE Laboratory, ENSA of Fez, Sidi Mohamed Ben Abdellah University, Fez, Morocco.*

[4] *EEIS Laboratory, ENSET of Mohammedia, Hassan II University of Casablanca, Mohammedia, Morocco.*

[5] *LAROSERI Laboratory, department of computer science, Faculty of Sciences, Chouaib Doukkali University, El Jadida, Morocco.*

[6] *EFSI Sarthe France.*

ARTICLEINFO

Article history

Received 20 Jan 2025
Accepted 22 Feb 2025
Published 20 Mar 2025

Keywords

IoT

Smart Buildings

Building Management Systems

Energy Management

Data Privacy

Security Blockchain

ABSTRACT

This literature review looks at the transformative impact of Internet of Things (IoT) technology on smart building management systems with a focus on enhancing operational efficiency, occupant safety, and comfort. As the number of IoT applications in the built environment increases, technology breakthroughs simplify and automate critical functions, including energy management, security, and environmental control. Despite all the advantages, such as the integration of the IoT with smart buildings, there are barriers, such as the compatibility of systems, scalability of infrastructure and data security and privacy issues in a connected ecosystem. This review examines some of those barriers and outlines potential solutions, such as standardized communication protocols, improved cybersecurity, and scalable, cost-effective IoT frameworks for existing and new buildings. The aim of the findings is to guide building owners, stakeholders, architects and urban planners in maximizing the benefits of IoT technology to create smarter, more sustainable and responsive buildings that support urban sustainability and foster better quality of life for tenants.

1. INTRODUCTION

In the past, the Internet of Things (IoT) was simply an older concept called Machine-to-Machine (M2M). M2M is an umbrella term for a series of wired or wireless network technologies that enable automatic data transfer between systems without the intervention of a human being [1]. The Internet of Things market is increasing at the global level, which encourages new participants to provide new technologies in multiple fields, such as computer hardware, network coverage and cloud connections, for data availability and storage. The Internet of Things (IoT) is often considered the next industrial revolution, and smart buildings have the potential to lead all use cases to "smart" maturity. Making things “smart” isn’t easy — and there are many protocols. The IoT in smart buildings consists of focusing on the connection of computer systems and internet-connected devices in construction structures to improve the management, comfort, safety, and efficiency of buildings [2].

As a critical component of smart buildings, the Internet of Things (IoT) transforms how spaces are managed and the experience of the occupants within them by allowing for the automation and control of lighting, heating, ventilation and security systems. Whether through energy management to reduce costs and carbon footprints, predictive maintenance to ensure that equipment is working as it should, or exception-based occupant experience customized environments, the IoT in smart buildings is a significant step toward smart homes and workplaces and more integrated living and working spaces. The inexpensive nature of IoT devices is because the processing and communication requirements and storage capacity are quite low compared with those of standard computing devices. It thus becomes easy and scalable to measure temperature and other environmental parameters in smart buildings. Because they rely on multiple hardware and software platforms, they are

*Corresponding author. Email: adnane.alkarkouri@uit.ac.ma

inherently heterogeneous. Fig. 1 shows the IoT infrastructure used for data-driven smart building operations and experimentation [3].

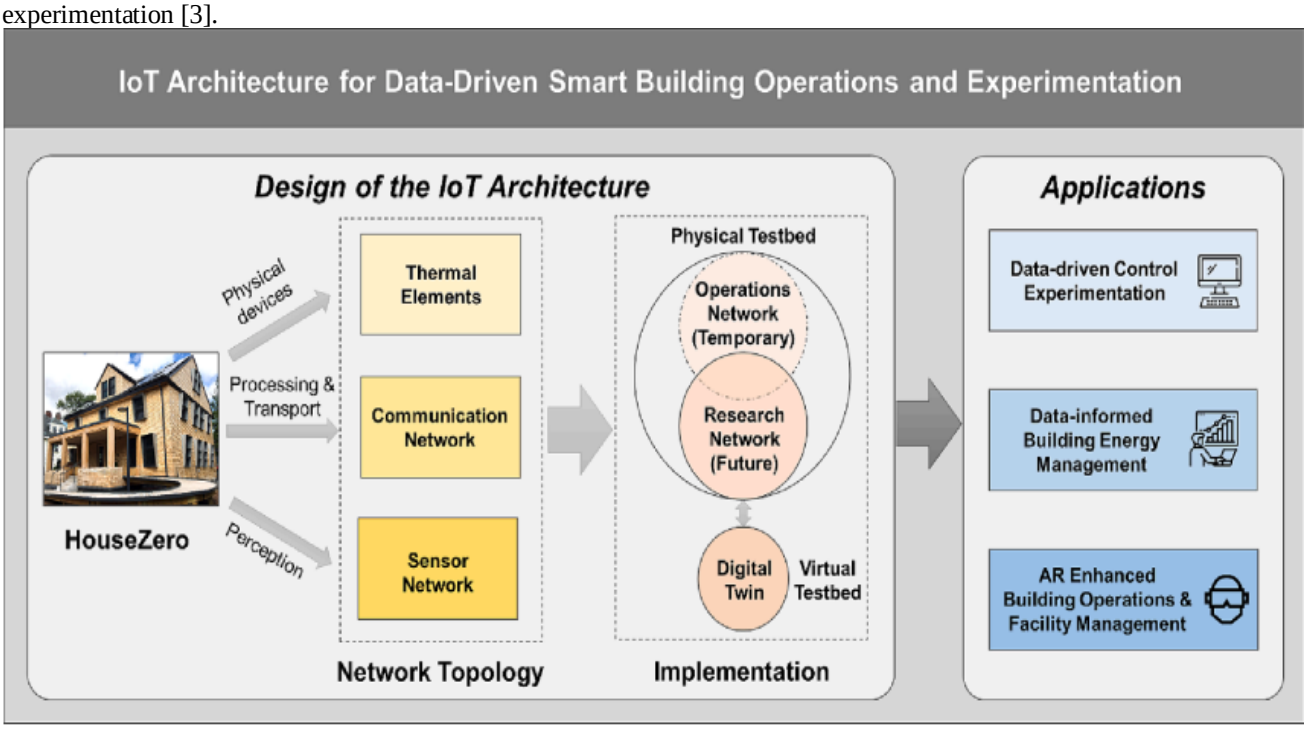

Fig. 1. IoT Architecture for Data-Driven Smart Building Operations and Experimentation

In the novel Internet of Things safety analysis within the smart home context, “smart home” appliances are those connected to a network, typically by Wi-Fi, including lights, TVs, air conditioners, ovens and refrigerators. Those homes are equipped with sophisticated automation and monitoring systems that allow appliances to be controlled via wristwatches or smartphones. Some buyers are fascinated by the notion of smart houses, whereas others are turned off by worries about security and the lack of backup plans if something goes awry. If the security of the building is compromised, an intruder could observe the building's occupants while they sleep or are away, subjecting them to the possibility of tremendous anxiety or physical restraint due to the manipulation of alarms or door locks. As we observed in the previous article, detecting homes resistant to these technologies can be the result of accidental use or purposeful attacks by malicious agents. Angelos Stavrou, an assistant professor of computer science at George Mason University, emphasized the need to avoid security approaches that would endanger the benefits that the Internet of Things can deliver. The remainder of the report focuses on this isolated incident [67][37].

In 2020, there were approximately 25 billion internet-linked devices. The reach of the enormous ecosystem referred to as the Internet of Things (IoT) encompasses far more than the usual range of desktop, laptop, and mobile devices. It encompasses home appliances, printers, cameras, wearable devices, etc.etc. These devices are connected to the network for user convenience and are often also stored with sensitive data. However, without user interfaces for installing security software, they are vulnerable and thus hard to secure. The Internet of Things (IoT) has the ability to transform future living and is seen to improve people’s lives; however, the IoT introduces a number of different security challenges that were not conceived when the internet was designed [38].

2. INTEGRATING FOG AND CLOUD COMPUTING FOR IOT IN SMART BUILDINGS

To maximize the development of the IoT in the context of smart linked buildings, two new paradigms were born as a result of the rapid increase in information and communication technologies: fog and cloud computing. To provide real-time data management and analytics at the network's edge, together with processing power and practically limitless storage in the cloud, it looks for an architecture that is more reactive, scalable, and efficient.

2.1 Fog and Cloud Computing in the IoT

2.1.1 Cloud Computing

Typically, located on local servers or personal computers, cloud computing hosts servers, storage, apps, and services via the internet or other distant locations. Sensor data are transmitted to the service layer for visualization after being stored in the cloud and are assessed by algorithms used for decision-making. Without the need for costly physical infrastructures, this technology enables both consumers and corporations to access their data and applications online. In the cloud, flexibility, scalability, and efficiency enable real-time resource access, enhanced teamwork, and substantial cost savings. Public, private, or hybrid cloud services can be used depending on needs and offer different security and management [4].

2.1.2 Fog Computing

"Computing in the fog" or fog computing is essential in areas with spotty internet service. To increase efficiency, the Internet of Things (IoT) decreases the amount of data sent to the cloud for processing, analysis, and storage. This is why data are processed close to their point of production on the edge of the network via fog computing. This enhances real-time decision-making for Internet of Things smart building applications without internet connections to the cloud, saves bandwidth, and reduces latency by removing transmission delays to a central cloud.
Computing in the "Fog" or "Cloud" moves processing power closer to the data source while centralizing data storage and processing. Both will see increased usage in smart building applications that leverage the Internet of Things to reduce energy costs, enhance the quality of life for tenants, and increase operational efficiency. The future of city life may depend on our collective efforts to make buildings smarter, more adaptive, and more environmentally friendly [5].

2.2 Data collection in smart buildings

2.2.1 Wireless sensor networks (WSNs)

Sensors capture data at the time of enabling data collection in a smart building system, and a WSN array of sensors is deployed [11]. Sensors are extremely important because they make real-time data available for automation and optimization systems in the environment. Two categories of sensors exist: dedicated sensors that are assigned to a specific application and are not shared with any other applications and nondedicated sensors that are sensors integrated into the users' smartphones and are not specific to any application, allowing users to participate at their convenience.

2.2.2 Radio frequency identification (RFID)

An integral part of the development of smart buildings is radio frequency identification (RFID), a technology that allows for communication with identified items. Smart buildings rely on radio frequency identification (RFID) technology, which provides useful tools to improve building security, resource management, occupant experience and operational efficiency. To achieve user-oriented, adaptive, and responsive buildings, their incorporation into a BMS is seen as a significant step forward [8].

3. WIRELESS TECHNOLOGIES FOR IOT IN SMART BUILDINGS

3.1 LoRa Technology

Internet of Things (IoT) devices may now communicate over great distances—up to several kilometers in densely populated areas—using a wireless communication technique called LoRa, which uses remarkably little energy. Owing to its ability to connect a myriad of sensors and devices, LoRa is ideal for long-term smart building applications that need to regulate and monitor factors such as temperature, lighting, security, and air quality. To deploy dense IoT networks effectively, which allows for better and more autonomous building management, LoRa's capacity to run over long distances without frequent battery replacements is critical [9].

3.2 Long Range Wide Area Network

The LoRaWAN (long-range wide-area network) is a type of wireless communication network in the field of the Internet of Things (IoT). This allows sensors and IoT devices across a building, or even remotely over multiple sites, to connect to a central network or the internet with a low-energy footprint. LoRaWAN is particularly suitable for the complex environments of smart buildings because of its extended range and ability to penetrate physical barriers such as walls [10].

3.3 Wireless Fidelity (WIFI)

Moreover, WIFI IEEE 802.11 (a standard developed for wireless technology, also known as the wireless local area network (WLAN)) is used in smart buildings to transmit the internet to many devices. Owing to its high performance, low-cost network, and simple technical implementation, WIFI is deployed in a smart building, supporting many WIFI connections and providing users with free internet access [11] [12].

3.4 ZigBee

ZigBee is incorporated based on IEEE 802.15.4. Typically, it is utilized to develop individual networks with applications and devices where lower data throughput, a protected network, and long battery life are mandatory. This makes it common in control and monitoring applications that require reliable data, minimal power consumption, and low cost. ZigBee is cheaper and simpler than other personal networks [9].

3.5 Bluetooth Low Energy

Bluetooth low energy (BLE) is a wireless technology that uses less power and is ideal for short-range communications; it is utilized in smart buildings to offer this connectivity. Owing to its moderate throughput and low latency, this technology is perfect for connecting inside IoT devices such as electronic locks, smart lighting, security systems, and temperature sensors. Because BLE and other wireless protocols, such as ZigBee and WiFi, use the same 2.4 GHz frequency band, interference between them must be carefully managed [12].

3.6 Sigfox

Hailing from 0--600 km UNB (ultra narrow band 0--600 km), Sigfox harnesses its proprietary UNB technology, offering an excellent communication solution to connect an array of low-energy IoT devices spanning long distances. Originally launched in 2009, Sigfox stands out for the wide coverage it provides over urban and rural locations, using very little power and with lower deployment costs. These features render it a very promising candidate for smart building applications, where the requirements for the connectivity to be reliable, economic, and scalable are very high [13].

3.7 LTE-M Technology

The advantages of LTE-M cellular technology for smart buildings include excellent connections, the fact that it does not necessitate any further infrastructure, and the fact that it is supported by an existing cellular network. Owing to their high penetrating capabilities, Internet of Things (IoT) devices have a long battery life because of their low power consumption and dependable communication, even in inaccessible areas. With its support for voice and data communications, LTE-M is an essential component of contemporary city design since it considerably improves smart building efficiency, security, and comfort [14].

3.8 Narrowband Internet of Things

NB-IoT (Narrowband Internet of Things) – A communication technology case for the Internet of Things sector, NB-IoT enables devices to connect within a wide LPWAN. NB-IoT is a simplified version of LTE designed and specified in the 3GPP specifications, corresponding to the 13th revision, Release 13, tailored for applications that necessitate wide network coverage, prolonged battery life for connected devices, and a considerable reduction in operational expenses. NB-IoT uses licenced frequency bands, typically from 7 MHz to 900 MHz, and features advanced transmission schemes that utilize OFDMA for downlink data and SC-FDMA for uplink information transportation. This makes NB-IoT one of the strongest solutions in the range from dense urbanity to countryside [14].

3.9 5th generation mobile network

Using tiny cells, millimeter waves, an SDMA, and a C-RAN, 5G can provide smart buildings with extremely high coverage areas, high throughput, and a well-managed network. These methods provide much higher bandwidths with extremely lower latencies and therefore enable highly advanced applications that enhance occupancy efficiency, safety, and comfort. 5G will be pivotal for the realization and evolution of smart buildings in more connected and intelligent urbanization [16].

3.10 6th generation mobile network

6G will truly be a paradigm shift in communication technologies with 6G-based systems performing orders of magnitude beyond the current 5G, and 6G will bring disruptive novelties to the design and functionality of smart buildings. This opens the door to hypermodern applications such as telesurgery and enhanced automation and augmented reality, all of which restore the unprecedented efficiency, safety, and comfort of buildings. Promising for efficiently performing very high-data-rate processing with low latency and to support interaction in and management with and of the built environment, 6G will lead buildings to evolve into highly integrated ecosystems, representing key transitions toward more futuristic and intelligent urbanization scenarios [14].

3.11 Comparison of Wireless Technologies

LoRa, NB-IoT, LTE-M, and ZigBee are four essential IoT technologies for long-range, low-power communication. This study analyses and compares them. Wireless technologies exhibit considerable diversity. LoRa technology is well suited for rural regions because of its range of 2--15 kilometers. In rural regions, NB-IoT has a range of 1--10 kilometers. ZigBees operate efficiently within a range of 10--100 metres. 6G is anticipated to surpass 5G in range owing to expected technology

advancements, although the range of 5G is significantly affected by the density of base stations. LTE-M is capable of covering medium--to-long distances, contingent upon local infrastructure.
NB-IoT and ZigBee have medium to high bandwidths, whereas LoRa has low bandwidth. 5G can provide high bandwidth, while 6G is expected to surpass it. Numerous IoT applications necessitate medium-bandwidth capabilities, which LTE-M may provide.
Energy consumption is also essential. LoRa is optimal for battery-limited devices because of its low power usage. ZigBee, NB-IoT, and LTE-M require reduced power consumption. 5G employs moderate to high optimized power for specific tasks, whereas 6G will utilize advanced technology for enhanced efficiency.
LoRa and ZigBee are optimal for various Internet of Things applications because of their low to moderate cost. NB-IoT and LTE-M are cost-effective. Nonetheless, the expenses associated with 5G infrastructure and execution are substantial, and the introduction of new technologies in 6G may exacerbate these costs.
Each of these technologies presents distinct deployment issues. LoRa and ZigBee are simpler to deploy and highly suitable for local networks. The moderate-complexity NB-IoT and LTE-M are contingent upon the cellular network design. Nonetheless, the sophisticated technology and spectrum management of 5G and 6G render them more complex. 6G will be intricate owing to novel standards and technology.
Interoperability significantly varies. Restriction to LoRa networks constrains compatibility. Zigbe seamlessly integrates with its ecosystem. 6G is anticipated to attain exceptional global interoperability, whereas NB-IoT, LTE-M, 5G, and 6G provide satisfactory to outstanding compatibility with existing and forthcoming cellular infrastructures.
These technologies frequently provide elevated security. NB-IoT and LTE-M exhibit superior security compared with LoRa and ZigBee because of their utilization of secure cellular networks. Owing to advancements in security technologies, compared with 5G, 6G may provide superior security.
These technologies have numerous uses. Long-range wireless technology is employed in smart cities, agriculture, and asset tracking. NB-IoT is suitable for industrial applications, asset tracking, and smart metering. ZigBees are extensively utilized in personal sensors, light industrial automation, and home automation. Smart city applications and asset tracking utilize LTE-M for mobile connectivity. 5G facilitates rapid mobile connectivity, the Internet of Things (IoT), augmented reality/virtual reality (AR/VR), and industrial applications. Ultimately, the diminished latency of 6G is expected to render it suitable for Internet of Things (IoT) applications, such as advanced augmented reality (AR) and virtual reality (VR), which require dependable and rapid communication.
LoRa is the unequivocal leader in low-power, long-range communication applications owing to its minimal installation costs. This technology is ideal for precision agriculture and asset tracking, which deploy devices across extensive distances.

4. POWERFUL COMMUNICATION PROTOCOLS IN THE IOT

Since smart buildings enable communication between numerous Internet of Things devices, communication strategies are crucial. Control over the building environment and effective management of demanding operations are made possible by these regulations.

4.1 Key Communication Protocols

4.1.1 Message queuing telemetry transport (MQTT)

Many smart building technologies, such as MQTT, use "publish subscribe" communication. It is different from any other protocol (including Ethereum). In this paradigm, data can move rapidly with minimal energy. We'll have more automation, energy management, security and periodic maintenance assistance. Adding devices is simple since the system is dependable and flexible. This increases efficiency, usability, and profitability. MQTT [18] is a requirement for intelligent building systems to be effective and economical.

4.1.2 Transmission Control Protocol (TCP)

The TCP is key to the safety and reliability of smart homes. Crucial details such as software updates and security protocols are provided accurately and organized. We need this internet control protocol (TCP) to transmit data over the internet safely. As such, building monitoring and control technologies are improving. The utility of this technology can ensure data flow [19]; therefore, smart building systems function accurately and are more reliable.

4.1.3 User Datagram Protocol (UDP)

The user datagram protocol (UDP) is ideal because of the speed and low latency demands of real-time smart building operations. This technology can be used for video surveillance and internal communication. TCP is more reliable, but UDP is required for video systems and fast replies. This optimizes the management of the temperature, alerts for security in addition to maximizing bandwidth [20].

4.1.4 Hypertext Transfer Protocol (HTTP)

The control systems of smart buildings are based on HTTP. This is because it is dependent on requests and responses. It enables internet-connected devices to converse with massive platforms. Computers make it possible for you to keep tabs on and manage infrastructure, making energy, security, and environmental management better. It will improve the user experience and operational efficiency [21] by making the building more user friendly to navigate.

4.2 Comparison of Communication Protocols

Table 1 provides a detailed comparison of four common IoT communication protocols. Each protocol has unique characteristics and is particularly adept at different scenarios. By understanding the key differences between MQTT, TCP, UDP and HTTP, one can determine which protocol is most appropriate for Internet of Things applications.

TABLE I. COMPARISON OF IOT COMMUNICATION PROTOCOLS

Protocol	Key Features	Use Cases
MQTT	Lightweight, publish-subscribe, low energy consumption	IoT applications, automation, energy management, security
TCP	Reliable, connection-oriented, secure	Data transmission, building monitoring and control
UDP	Connectionless, low latency	Real-time applications, video monitoring, internal communication
HTTP	Request-response, supports TLS/SSL	Web communication, infrastructure monitoring and control

Specific requirements imply that IoT protocols have various features and use cases. MQTT is lightweight-oriented and follows a publish-subscribe model, making it ideal for energy-oriented IoT applications (such as smart houses (bulbs, thermostats and sensors) [60], industrial IoT (release of data between machines (low-bandwidth environments) [61]) and Smart City [62]-[63]. Since the transmission control protocol (TCP) provides reliable, connection-oriented services, it has applications in monitoring and control, including building automation (e.g., reliable transfer of information between HVAC systems and centralized monitor software) and the healthcare IoT (e.g., secure transfer from medical devices into cloud-based health information systems) [64]. In contrast, the UDP provides a connectionless and low-latency mechanism, which makes it suitable for real-time applications, such as video streaming in surveillance systems and multiplayer game applications powered by the IoT [65]. Finally, given its intrinsic request–response model and support for TLS/SSL, HTTP is better applicable for web communication and infrastructure monitoring, e.g., certain smart parking systems or the relay of data from dams and bridges to a web-based dashboard [66].

4.3 Choosing the Right Protocol

When assessing the requirements of an IoT (internet of things) application, it is important to weigh both the positives and negatives of each standard. The cost, setup complexity, energy consumption, and range are all considered.

Each protocol has its own properties in regard to networked systems. MQTT, TCP, UDP, and HTTP are distinct protocols, and each best fits certain use cases. MQTT stands for "Message Queuing Telemetry Transport," and it is a messaging system designed to allow devices to communicate in an efficient and reliable way. Its publish-subscribe mechanism does wonder when there is no need for constant connection. MQTT is very stable and has different quality-of-service (QoS) options for devices to manage message delivery according to the environment. This protocol is the perfect solution for low-bandwidth connection situations, as it is TLS/SSL secure and requires little network bandwidth for communication. It is widely used for IoT, home automation and monitoring applications because of its low data transfer capacity and low latency [18].

The transmission control protocol (TCP) provides secure and reliable communication between devices. It is one of the internet's foundational protocols. If the message is exchanged via a connection, a connection is performed and maintained throughout the communication session. In TCP, all the data are sent in the form of messages, rearranging the packets and controlling the flow. It provides encryption via transport layer security (TLS) and secure socket layer (SSL) to transmit secure data. It uses bandwidth according to the case of the application. Further detailed descriptions regarding the usage of TCP as a reliable communication protocol with medium latency are suitable for applications such as web browsing and file downloads [19].

The user datagram protocol (UDP) is a connectionless transport protocol that sends the data without establishing a connection. This offers low latency but with no error checking or retransmission, making it less reliable than the TCP. The security of the UDP relies on the software that uses it. It is lightweight because of its small footprint and low to medium bandwidth requirements. UDP is used in video streaming, online gaming and VoIP applications, in which speed is critical [20].

HTTP is an application-layer protocol based on a request–response model. It uses TCP or UDP to transmit data and can use TLS/SSL to encrypt communication. One of the primary reasons for relatively high data use is the use of HTTP headers, which, compared with other communication methods, require many transfers. However, the protocol is also able to support

complex transactions throughout the web and emphasize relational data management structures. For this reason, HTTP is a good candidate for REST-ful services and web browsing. Since every protocol serves different requirements and environments, it is important to choose an adequate protocol for data communication and transmission [21].

5. INTEGRATION OF BLOCKCHAIN AND THE IOT

5.1 Overview of Blockchain

Essentially, blockchain allows a wide range of stakeholders to interact and transact without needing trust—that is, if there is no middleman. We call a "trustless" transitive state machine for this reason. However, the drawback of entrusting a platform to a centralized authority is the inefficiency caused by the expense of a middleman. Compliance (to prevent misuse of public trust) and the expense of the IT systems to handle the regulation are quite expensive. The global cost of financial services regulatory compliance is USD 1.7 trillion, of which 18% is waste. Because of the opaqueness caused by wrongdoing, the indirect costs are higher; for a Ponzi scheme, the investors lose half of that amount. The business logic becomes opaque to all except for the participants, and only the cryptographic hashes of the transactions need to be disclosed to regulatory bodies so that they can assess their relevance to regulatory oversight. In the event that there is a case where an inquiry of a business failure is pursued, the ledger of the transactions helps minimize the cost in tracing back the issue. Decentralization is another vital property of blockchain. With more global regulations coming, there is a greater need for data sovereignty, where a person's data must reside within the geography of that person. In the current state of IT systems, data storage is centralized, and highly sophisticated segmentation of data storage systems is needed to comply with data sovereignty regulations, particularly in cloud-based systems. On a private chain, decentralized storage is a straightforward data sovereignty solution, whereas a public chain is implicitly data sovereignty compliant. IoT device data do not have to 'cross the pond' to perform a transitive state on a centralized system in another geographic area[68][22].

5.2 Intersection of the blockchain and IoT

One can now build a supply chain network on the blockchain via smart contracts and systems that are comparable to IBM's latest blockchain-based supply chain solution. When certain circumstances are satisfied, smart contracts can automatically execute the terms that were defined between the parties. A smart contract transaction can record an occurrence involving a change in ownership, leaving an immutable and transparent record on the blockchain [23].

The capacity to offer transparency and an audit trail is another advantage of blockchain. Internet of Things (IoT) systems that monitor the flow of commodities throughout a supply chain greatly benefit from this function. There is usually much paperwork, and many parties involved when products are transferred through a system. Because of the added complexity and work involved, mistakes in recording modifications and determining who made them are common [24].

These solutions are more secure with blockchain because of its decentralized nature. The additional security measures needed to safeguard data on a cloud server are diminished as a result of data not being kept in a single repository. Only the data that devices are now using are briefly retained, and these data are stored directly on the blockchain. Furthermore, smart contracts guarantee the proper execution of automation choices [25].

Data sharing increases the risk that one device may act upon faked information received from another, which could have unintended consequences. In addition to endangering the system's integrity, attacks or alterations to the data source could damage the decision-making process that relies on these data [26].

All of the components in an Internet of Things (IoT) home automation system communicate with one another and exchange data. Information about inhabitants, including their security choices, may be stored in such a system. The intelligent components of the system automatically decide what to do with the data at their disposal. This raises the bar for hostile actors and adds another layer of complexity [27].

The decentralized nature of blockchain security is a major selling point for implementing it in Internet of Things (IoT) systems. Research has shown that a private Ethereum blockchain can effectively simulate and prevent attack scenarios on Internet of Things (IoT) home automation systems [28].

A safe environment can be achieved through the combination of blockchain technology and the Internet of Things. Researchers have reported that blockchain significantly increases IoT system resilience to assaults at different levels. Device monitoring and interference, data theft, and other forms of cyberattack are all part of these assaults [29].

5.3 Benefits of Combining Blockchain and IoT

Another cost-cutting measure is IoT device reputation. This is accomplished by attestation, which verifies device identity against an authority. Maintaining this trust operation is expensive. The history of an immutable ledger can demonstrate device capacity and service quality to establish a reputation [29]. The use of blockchain smart contracts illustrates this. Smart contracts are coded agreements that self-execute. Automation can replace the human oversight of procedures. This eliminates the cost of a supervisory authority and reduces the degree of trust between parties with an intermediary. Real-world examples include utility smart contracts for IoT devices to automate electricity payments. This would be easier and cheaper to operate

than the existing invoicing system and might save end users money by passing on decreased service provider charges [30]. We know that cost is the greatest obstacle to IoT device development. Running a decentralized device system is expensive because of trust and upkeep. This is where blockchain helps. The secure and permanent record can be used by IoT devices for automation. Blockchain reduces IoT expenses by removing overhead and improving efficiency [28]. Blockchain is generally considered a problem solver. The technology is young; therefore, many use cases are theoretical. This is not true for blockchain-IoT integration. This use case is likely to arise since the two technologies solve problems. Blockchain technology can solve IoT efficiency difficulties. Blockchain technology can help the IoT reduce cost, complexity, security, trust, and efficiency [28].

5.4 Data Security and Privacy in IoT

Data security is commonly regarded as a robust companion to data privacy. However, the introduction of the IoT poses a double-edged sword to this partnership. On the one hand, the proliferation of various types of endpoints generating data creates a breeding ground for emerging and established cyber threats. In contrast, IoT devices are specifically built to collect additional information that can be used for increased automation as well as for enabling decision-making. However, unless the information falls into the wrong hands, the mass collection of data is an invasion of privacy. This leads to the potential tendency for law enforcement profiling and discriminating against people according to their data. Existing regulations, such as the GDPR, that seek to prevent those issues prove that data privacy is a core question in the progress of the IoT. However, this data-oriented characteristic of the IoT poses difficult problems in ensuring that private data are protected and that access to private data is controlled. Traditional approaches to IT data protection (building walls and encrypting databases) should be abandoned, outdated, and not suitable for the secure distributed data storage and transmission system that is most effectively implemented through the combination of the blockchain and the IoT [31].

5.5 Potential impact of the blockchain on the IoT

Blockchain technology would also greatly improve the proof of identity and the autonomy of the device. Currently, devices are becoming smarter and more autonomous, but with this, there are threats since the devices are still controlled by a central authority. Devices will require a system to monitor interactions with other devices and ensure that the other gadget is functioning in the owner's best interest and will not hurt them if they are to have more autonomy. Data policies can be formalized, and a blockchain can record metadata so that devices are assured from these policies and transact in an unbiased manner[67][32]. A blockchain is a distributed database that maintains a list of records in a secure and permanent fashion. Once recorded, that transaction cannot be altered. Breaking it down like this could be massively valuable in the IoT space. With the help of a smart contract, a basic device can communicate with another device and carry out the conditions of the agreement without the need for human interaction. The blockchain has a record of the entire procedure. This eliminates many of the inefficiencies involved in conducting business while introducing accountability and traceability. Devices would know that the value they have exchanged is secure, and they might exchange value with each other in the form of microdata payments (for which no human input is required) [33].

5.6 Emerging Trends in Blockchain and IoT Integration

In contrast, consortia or single businesses will host dedicated chains to deliver tightly integrated solutions for specific problems or vertical markets. Current work by SMEs on Ethereum-based smart contract solutions may involve logical evolution. This method may dominate technology utilization in the future [34].

Flexible and hybrid integration of on-chain and off-chain architectures, including traditional databases, will emerge. This is because a wholesale switch to on-chain solutions is neither practicable nor economically viable, and many IoT devices require off-chain and conventional processing and storage. Large industrial device data files can be stored in an offsite cloud data store, unlike device management data, which can be committed to an on-chain ledger. Flexible integration requires gateway systems to translate protocols between systems and off-chain/on-chain domains [35].

Multiple-purpose designs that solve multiple challenges will be most common and profitable. They use multichain designs, which are linked or siloed blockchain systems. Only the simplest implementations use one chain. Like multimode architecture solutions used to integrate systems, affordability and the aim of leveraging current systems and making them interoperable with minimal disturbance are the main considerations. Filament, which builds blockchain solutions for the industrial internet, announced that it would switch from a public ledger to a multichain approach to reduce costs and scale. The IOTA project is developing a more ambitious scenario with Tangle, a flexible and modular multichain data structure that can interface with standard blockchains [36].

5.7 Strategies for Enhancing Security in the IoT for Blockchain

The IoT devices are arranged in a secure network topology via this technique. IoT devices with the same degree of security clearance are grouped into a subnetwork, and a firewall is used to keep the network isolated from another subnetwork. The data transmission between IoT devices will be better managed by dividing them into a subnetwork, and the degree of

security will be effectively implemented since it can be modified on the basis of the security clearance level. Furthermore, to improve the security of data transmission between IoT devices, end-to-end encryption needs to be implemented in the topology [39].

- **Secure Topology**

A secure topology involves structuring the IoT network to minimize vulnerabilities and enhance security resilience. The IoT for blockchain can include isolating critical components, enforcing network segmentation, and using access control to restrict unauthorized devices and activities. By carefully designing the topology, the system can prevent certain security threats from propagating throughout the network [40].

- **Prevention Strategy**

Prevention strategies are proactive measures designed to reduce the likelihood of security issues in IoT systems that use blockchain. These strategies include implementing strong authentication protocols, data encryption, and network monitoring to identify and mitigate potential threats before they can affect the system. Prevention and detection strategies work in tandem, with prevention aiming to thwart attacks before they occur and detection strategies identifying security breaches in real time [41].

6. INTERPRETING OUR FINDINGS

IoT technologies embedded into smart buildings could transform our engagement with our built environments and their administration. IoT sensors and devices can create buildings that are more responsive to occupants, greener and more energy efficient. There are many possibilities, ranging from enhanced comfort and safety to efficient energy use. Nonetheless, the success of smart buildings with the IoT relies on communication technologies that facilitate the smooth transfer of information and interoperability between systems and devices.

Networked Horizons: Communication technologies will shape the future growth of smart buildings. As the Internet of Things environment continues to develop, standardized protocols encouraging interoperability across platforms and devices are necessary. In particular, the most developed standards in this field are protocols, such as MQTT, CoAP and OPC UA, that can ensure secure and effective communication in smart buildings.

The capabilities of smart building IoT devices could be improved further through edge computing and machine learning, leading to smarter and more autonomous devices. Some of the machine learning algorithms running and processing incoming data closer to the source acquire real-time insights and predictive insights, allowing them to manage the process more proactively and dynamically.

The next-generation technology, 5G, could help in the faster adoption of the IoT in smart buildings. Its ultrafast, low-latency connection could enable the building of more controllable communication networks. This will allow for more seamless integration between IoT devices and new applications, including virtual assistants and augmented reality, into building settings.

Edge computing, artificial intelligence, fifth-generation wireless networks and advanced communication protocols promise to take the smart building IoT to new heights. These advances will make ecosystems more interconnected, intelligent, and sustainable. These IoT-based solutions help drive operational efficiency, increase resource utilization, and ensure citizens' QoL.

Many elderly devices could support Ethereum's future PoS consensus. If the PoS system is fully operational, lightweight Ethereum clients might become possible for devices within such use cases. It will be tested against a case study of a simulated botnet and other attacks on a simulated IoT environment to explore its robustness against current vulnerabilities.

This forms a compelling argument for a new architecture to mitigate these vulnerabilities with the integration of blockchain. This architecture would need more design and development that would allow resource-constrained IoT devices to play a part in blockchain protocols. In doing so, such a framework could be revolutionary, transferring IoT resources to child chains nested in a larger blockchain network while securing these data in an automated, cost-effective manner.

The analysis scales blockchain’s benefits to IoT modules against prevalent security threats, particularly DDoS attacks. It provides a basic understanding of all these issues via the Kill chain and the attack tree model. An annotated taxonomy is proposed to pinpoint different types of security threats and vulnerabilities during various stages. The motivations and mechanics of such attacks have been described well enough to allow effective countermeasures to be developed, many of which are already possible when a blockchain is used.

We discuss the idea of blockchain in the IoT and discuss the security impacts of blockchain along with critical vulnerabilities. We present an overview of new blockchain technology and its present usage in the IoT, establishing a path for the best utilization of its attributes. Further works will perform a more in-depth analysis of the proposed architecture, its resolution schemes, and the resilience of the architecture regarding a varying range of possible attacks. A comprehensive theoretical analysis and practical implementation will substantiate these results. The table below shows a comparative study.

TABLE II. COMPREHENSIVE ANALYSIS AND COMPARATIVE THEORETICAL AND PRACTICAL STUDY

REFERENCE	AUTHORS	YEAR	TITLE	KEY POINTS	LIMITATIONS	KEY FINDINGS
[42]	Z. RAHMAN, X. YI, I. KHALIL, A. KELAREV	2021	BLOCKCHAIN FOR IOT: A CRITICAL ANALYSIS CONCERNING PERFORMANCE AND SCALABILITY	ANALYSIS ON PERFORMANCE AND SCALABILITY ISSUES IN BLOCKCHAIN FOR IOT	LIMITED PRACTICAL APPLICATION DUE TO EARLY-STAGE TECHNOLOGY; HIGH COMPUTATIONAL COST	IDENTIFIES BOTTLENECKS IN BLOCKCHAIN SCALABILITY AND PERFORMANCE WITHIN IOT APPLICATIONS
[43]	B. MACHADO AGOSTINHO, M.A. RIBEIRO DANTAS, A.S.R. PINTO	2021	PROPOSAL OF AN ECONOMY OF THINGS ARCHITECTURE AND AN APPROACH COMPARING CRYPTOCURRENCIES	DISCUSSES THE ECONOMIC ASPECTS AND COMPARISON OF CRYPTOCURRENCIES WITHIN IOT	LIMITED TO CONCEPTUAL FRAMEWORKS, LACKS EMPIRICAL VALIDATION	PROPOSES ARCHITECTURE FOR ECONOMY-BASED IOT, EMPHASIZING CRYPTOCURRENCY COMPARISON
[44]	H. DHIA ZUBAYDI, P. VARGA, S. MOLNÁR	2023	LEVERAGING BLOCKCHAIN TECHNOLOGY FOR ENSURING SECURITY AND PRIVACY ASPECTS IN INTERNET OF THINGS	SYSTEMATIC REVIEW ON SECURITY AND PRIVACY ENHANCEMENTS THROUGH BLOCKCHAIN IN IOT	CHALLENGES IN IMPLEMENTING UNIFORM SECURITY PROTOCOLS ACROSS IOT DEVICES	HIGHLIGHTS HOW BLOCKCHAIN CAN STRENGTHEN SECURITY AND PRIVACY IN IOT SYSTEMS
[45]	M. ANSARI, S. ARSHAD ALI, M. ALAM	2019	A SYNERGISTIC APPROACH FOR INTERNET OF THINGS AND CLOUD INTEGRATION: CURRENT RESEARCH AND FUTURE DIRECTION	FOCUSES ON INTEGRATION STRATEGIES FOR IOT AND CLOUD WITH BLOCKCHAIN TECHNOLOGY	LIMITED FOCUS ON REAL-WORLD DEPLOYMENT AND SCALABILITY CONCERNS	SUGGESTS A UNIFIED IOT-CLOUD-BLOCKCHAIN INTEGRATION MODEL FOR EFFICIENCY
[46]	N. AZIZI, H. MALEKZADEH, P. AKHAVAN, O. HAASS ET AL.	2021	IOT–BLOCKCHAIN: HARNESSING THE POWER OF INTERNET OF THING AND BLOCKCHAIN FOR SMART SUPPLY CHAIN	EXAMINES THE APPLICATION OF BLOCKCHAIN FOR ENHANCING SUPPLY CHAIN MANAGEMENT THROUGH IOT	SCALABILITY AND LATENCY ISSUES IN REAL-TIME DATA TRACKING	DEMONSTRATES IMPROVED TRACEABILITY AND SECURITY IN SUPPLY CHAINS
[47]	M. MAJID AKHTAR, D. RAZA RIZVI, M. ABDUL AHAD, S.S. KANHERE ET AL.	2021	EFFICIENT DATA COMMUNICATION USING DISTRIBUTED LEDGER TECHNOLOGY AND IOTA-ENABLED INTERNET OF THINGS FOR A FUTURE MACHINE-TO-MACHINE ECONOMY	DISCUSSES DISTRIBUTED LEDGER TECHNOLOGIES FOR IMPROVED DATA COMMUNICATION IN IOT	LIMITED TESTING IN PRACTICAL M2M ENVIRONMENTS	FINDS IOTA AND DLT EFFECTIVE FOR HIGH-SPEED, DECENTRALIZED IOT COMMUNICATION
[48]	L. HANG, D.H. KIM	2019	DESIGN AND IMPLEMENTATION OF AN INTEGRATED IOT BLOCKCHAIN PLATFORM FOR SENSING DATA INTEGRITY	DESCRIBES AN IOT BLOCKCHAIN PLATFORM AIMED AT ENSURING DATA INTEGRITY	HIGH RESOURCE REQUIREMENTS, MAKING IT LESS FEASIBLE FOR LOW-POWER DEVICES	SHOWS HOW BLOCKCHAIN CAN MAINTAIN DATA INTEGRITY IN IOT
[49]	S. KUMAR SINGH, S. KUMAR	2021	BLOCKCHAIN TECHNOLOGY: INTRODUCTION, INTEGRATION AND SECURITY ISSUES WITH IOT	PROVIDES A GENERAL OVERVIEW OF BLOCKCHAIN TECHNOLOGY AND ITS SECURITY IMPLICATIONS FOR IOT	PRIMARILY A THEORETICAL DISCUSSION, LACKS PRACTICAL INSIGHTS	INTRODUCES SECURITY CHALLENGES AND POTENTIAL SOLUTIONS FOR IOT-BLOCKCHAIN INTEGRATION
[50]	C.H. WU, Y.P. TSANG, C. KA-MAN LEE, W.K. CHING	2021	A BLOCKCHAIN-IOT PLATFORM FOR THE SMART PALLET POOLING MANAGEMENT	IMPLEMENTATION OF A BLOCKCHAIN-IOT PLATFORM FOR LOGISTICS AND PALLET MANAGEMENT	COST AND COMPLEXITY OF DEPLOYING BLOCKCHAIN IN LOGISTICS	DEMONSTRATES ENHANCED LOGISTICS TRACKING AND ACCOUNTABILITY THROUGH IOT BLOCKCHAIN

[51]	M.R. Alagheband, A. Mashatan	2022	Advanced encryption schemes in multitier heterogeneous internet of things: taxonomy, capabilities, and objectives	Study on encryption methods suitable for multitier IoT systems	Resource-intensive encryption not always suitable for IoT constraints	Offers a taxonomy of encryption schemes for secure IoT
[52]	J. Antonio Guerra, J. Ignacio Guerrero, S. Garcia, S. Dominguez-Cid et al.	2022	Design and Evaluation of a Heterogeneous Lightweight Blockchain-Based Marketplace	Evaluation of a lightweight blockchain solution for IoT marketplace applications	Limited by transaction speed and data storage capacity	Provides a low-cost blockchain solution tailored for IoT marketplaces
[53]	M. Maroufi, R. Abdolee, B. Mozaffari Tazekand	2019	On the Convergence of Blockchain and Internet of Things (IoT) Technologies	Discusses the theoretical and practical aspects of integrating blockchain with IoT	General focus, lacking specific application cases	Summarizes the potential benefits and technical challenges of IoT-blockchain convergence
[54]	B. Xie, Q. Zhang, J. Qin	2019	Joint Optimization of Cooperative Communication and Computation in Two-Way Relay MEC Systems	Looks into the optimization of communication and computation in IoT systems	Limited focus on blockchain integration	Optimizes IoT communication, potentially beneficial for blockchain
[55]	A. Kumar Tyagi, S. Dananjayan, D. Agarwal, H. Farhana Thariq Ahmed	2023	Blockchain—Internet of Things Applications: Opportunities and Challenges for Industry 4.0 and Society 5.0	Discusses the opportunities and challenges of blockchain IoT applications in modern industry and societal contexts	High costs associated with blockchain infrastructure	Explores new IoT-blockchain applications in Industry 4.0
[56]	A. Alkhateeb, C. Catal, G. Kar, A. Mishra	2022	Hybrid Blockchain Platforms for the Internet of Things (IoT): A Systematic Literature Review	Systematic review of hybrid blockchain platforms designed for IoT	Lacks empirical testing of hybrid models	Highlights the strengths and limitations of hybrid blockchain in IoT
[57]	R. Zhang, C. Xu, M. Xie	2022	Secure Decentralized IoT Service Platform using Consortium Blockchain	Focus on the use of consortium blockchain for securing decentralized IoT services	Potential issues in interoperability across IoT systems	Demonstrates consortium blockchain as a secure solution for IoT
[58]	Hari Mohan Rai	2024	Enhanced Security Protocols for Blockchain-IoT Ecosystems in Urban Infrastructures"	Examines advanced security protocols to mitigate vulnerabilities in IoT networks integrated with blockchain	High computational demand may limit practical applications in resource-constrained IoT devices	Shows enhanced security resilience in blockchain-IoT systems, especially for urban applications
[59]	Prabhat Kumar	2024	Digital twin-driven SDN for smart grid: A deep learning integrated blockchain for cybersecurity	Focuses on decentralized energy management using blockchain in IoT-enabled smart grids	Limited adoption due to high initial setup costs and complexity	Demonstrates potential for significant energy savings and reliability improvements in smart grids with IoT and blockchain integration

7. CONCLUSION AND PERSPECTIVES

Smart building security systems powered by IoT technology have immense potential for automation, real-time monitoring, and improving operational efficiency. However, Internet of Things (IoT) networks are interconnected so much that they pose new security threats that require strong solutions. Blockchain has emerged as a potential solution to these issues since its decentralized, immutable, and transparent framework can be used to improve the availability, integrity, and confidentiality of smart building data. The implementation of blockchain can allow smart buildings to develop more resilient security frameworks that lessen the risk of unauthorized access, authorize secure data exchanges between devices, and improve trust in all the various parties involved.

This review highlights several important issues for future research and practical approaches. The scalability of blockchain in large IoT ecosystems is one of the main obstacles to overcome in this area. Existing forms of blockchain models tend to be computationally intensive and energy-consuming and, as such, may be ineffective in large, dynamic smart building ecosystems. To fill this gap, it is vital to create blockchain models that consume less energy. Moreover, hybrid frameworks, which utilize blockchain in combination with innovative technologies, in the areas of edge computing and artificial intelligence, potentially accelerate security, scalability and performance under the constraints of limited resources. Such hybrid approaches would enable more efficient data processing nearer the data source with the added benefit of the blockchain's security advantages.

Furthermore, smart building blocks need practical, real-world implementation testing of blockchain-enabled Internet of Things (IoT) frameworks to ensure that they do not become lidi in use cases that must live up to constantly changing conditions. Evaluating these systems in controlled environments is a necessary step to determine how to keep these systems operational in real time, as one must address performance ceilings while adapting to the pressures of operational resilience. The insights gained from empirical studies can help to identify practical challenges, limitations, and opportunities for using these frameworks, which can, in turn, aid in refining blockchain-enabled IoT solutions for real-world applications.

In the future, IoT and blockchain technology integration in smart building security systems can provide significant opportunities, including automation, real-time monitoring and operational efficiency; however, there are also challenges, which must be addressed through innovative solutions. Thus, future investigations should aim at scalable and energy-efficient blockchain designs for large-scale IoT setups, including low-energy consensus algorithms. The integration of edge computing with blockchain and AI can lead to improved processing efficiency of data as well as predictive threat detection, whereas adaptive security measures can be modified in real time according to evolving vulnerabilities. For cross-platform interoperability, interoperability standards and protocols must be established, and legacy systems must be updated to include blockchain capabilities. Importantly, advanced cryptographic primitives, as well as compliance-oriented smart contracts, could enhance privacy and data protection, whereas field tests are needed to determine the real-world performance of the systems under nonstatic conditions. These, combined with the focus on user-friendly interfaces, sustainability, and the economic feasibility of systems, will facilitate the adoption of blockchain-enabled IoT systems to ensure that cities become safer, smarter, and more sustainable. However, this fusion introduces additional obstacles that demand creative resolutions. Several specific directions for future research can be identified on the basis of the current status of research and implementation.

Future Research Questions

1. Hybrid Frameworks
    - How can edge computing be effectively integrated with blockchain to increase data processing efficiency in smart building IoT networks?
    - What AI algorithms can be developed to work in tandem with blockchain for predictive security threat analysis in smart buildings?
2. Real-World Testing and Implementation
    - What are the performance metrics and benchmarks for evaluating blockchain-enabled IoT systems in operational smart buildings?
    - How do Blockchain-IoT frameworks perform under various stress conditions, such as high network traffic or attempted security breaches?
3. Adaptive Security Measures
    - Can machine learning models be developed to dynamically adjust blockchain security parameters on the basis of real-time threat assessments in smart buildings?
    - How can blockchain-based access control systems be designed to accommodate the fluid nature of smart building occupancy and usage patterns?

By addressing these research questions, the scientific community can contribute to the development of more robust, efficient, and practical blockchain-IoT security solutions for smart buildings. This research will be crucial in realizing the full potential of these technologies in creating safer, more sustainable, and more responsive urban environments.

Conflicts of interest

The authors confirm that the material provided is original and has not been published in another publication for review.

Funding

No government, corporate, or nonprofit entity provided a particular grant for this research.

Authors' Contributions:

All the authors contributed equally to the composition of this research study.

Acknowledgement

We thank the participants who contributed their touch dynamics data to this study.

REFERENCES

[1] R. Sudarmani, K. Venusamy, S. Sivaraman, P. Jayaraman, K. Suriyan, and M. Alagarsamy, "Machine to machine communication enabled internet of things: A review," International Journal of Reconfigurable and Embedded Systems, vol. 11, no. 2, pp. 126, 2022.

[2] B. Dong, V. Prakash, F. Feng, and Z. O'Neill, "A review of smart building sensing system for better indoor environment control," Energy and Buildings, vol. 199, pp. 29-46, 2019.

[3] A. Malkawi, S. Ervin, X. Han, E. X. Chen, S. Lim, S. Ampanavos, and P. Howard, "Design and applications of an IoT architecture for data-driven smart building operations and experimentation," Energy and Buildings, vol. 295, no. 113291, 2023.

[4] E. Carrillo, V. Benitez, C. Mendoza, and J. Pacheco, "IoT framework for smart buildings with cloud computing," in Proc. IEEE First International Smart Cities Conference (ISC2), pp. 1-6, 2015.

[5] F. J. Ferrández-Pastor, H. Mora, A. Jimeno-Morenilla, and B. Volckaert, "Deployment of IoT edge and fog computing technologies to develop smart building services," Sustainability, vol. 10, no. 11, pp. 3832, 2018.

[6] A. Maatoug, G. Belalem, and S. Mahmoudi, "Fog computing framework for location-based energy management in smart buildings," Multiagent and Grid Systems, vol. 15, no. 1, pp. 39-56, 2019.

[7] H. Ghayvat, S. Mukhopadhyay, X. Gui, and N. Suryadevara, "WSN-and IoT-based smart homes and their extension to smart buildings," Sensors, vol. 15, no. 5, pp. 10350-10379, 2015.

[8] F. Alshahrany, M. Abbod, and I. Moualek, "WSN and RFID integration to support intelligent monitoring in smart buildings using hybrid intelligent decision support systems," Acta Physica Polonica A, vol. 128, no. 2B, 2015.

[9] A. I. Ali and S. Z. Partal, "Development and performance analysis of a ZigBee and LoRa-based smart building sensor network," Frontiers in Energy Research, vol. 10, pp. 933743, 2022.

[10] A. S. Shaker, "A survey of smart buildings and homes using low-power wide-area network (LoRa WAN)," in Proc. 2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), pp. 1-7, 2020.

[11] H. Zou, Y. Zhou, H. Jiang, S. C. Chien, L. Xie, and C. J. Spanos, "WinLight: A WiFi-based occupancy-driven lighting control system for smart building," Energy and Buildings, vol. 158, pp. 924-938, 2018.

[12] G. D. Putra, A. R. Pratama, A. Lazovik, and M. Aiello, "Comparison of energy consumption in Wi-Fi and bluetooth communication in a Smart Building," in Proc. IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), pp. 1-6, 2017.

[13] W. Xu, J. Zhang, J. Y. Kim, W. Huang, S. S. Kanhere, S. K. Jha, and W. Hu, "The design, implementation, and deployment of a smart lighting system for smart buildings," IEEE Internet of Things Journal, vol. 6, no. 4, pp. 7266-7281, 2019.

[14] K. V. Deshpande and A. Rajesh, "Investigation on imcp based clustering in LTE-M communication for smart metering applications," Engineering Science and Technology, an International Journal, vol. 20, no. 3, pp. 944-955, 2017.

[15] Y. Li, X. Cheng, Y. Cao, D. Wang, and L. Yang, "Smart choice for the smart grid: Narrowband Internet of Things (NB-IoT)," IEEE Internet of Things Journal, vol. 5, no. 3, pp. 1505-1515, 2017.

[16] T. Mazhar, M. A. Malik, I. Haq, I. Rozeela, I. Ullah, M. A. Khan, and H. Hamam, "The role of ML, AI and 5G technology in smart energy and smart building management," Electronics, vol. 11, no. 23, pp. 3960, 2022.

[17] S. Dang, G. Ma, B. Shihada, and M. S. Alouini, "Smart Buildings Enabled by 6G Communications," arXiv preprint arXiv:1904.07959, 2019.

[18] A. Ramelan, F. Adriyanto, B. A. C. Hermanu, M. H. Ibrahim, J. S. Saputro, and O. Setiawan, "IoT based building energy monitoring and controlling system using LoRa modulation and MQTT protocol," in IOP Conference Series: Materials Science and Engineering, vol. 1096, no. 1, p. 012069, 2021.

[19] A. Kumar, S. Sharma, N. Goyal, A. Singh, X. Cheng, and P. Singh, "Secure and energy-efficient smart building architecture with emerging technology IoT," Computer Communications, vol. 176, pp. 207-217, 2021.

[20] A. Nugur, M. Pipattanasomporn, M. Kuzlu, and S. Rahman, "Design and development of an IoT gateway for smart building applications," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 9020-9029, 2019.

[21] M. Javaid, A. Haleem, R. P. Singh, R. Suman, et al., "A review of Blockchain Technology applications for financial services," in Benchmarks, Standards, 2022.

[22] F. Dietrich, D. Palm, and L. Louw, "Smart contract based framework to increase transparency of manufacturing networks," Procedia CIRP, 2020.
[23] M. Liu, A. Robin, K. Wu, and J. Xu, "Blockchain's Impact on Accounting and Auditing: A Use Case on Supply Chain Traceability," Journal of Emerging Technologies, 2022.
[24] J. Zarrin, H. Wen Phang, L. Babu Saheer, and B. Zarrin, "Blockchain for decentralization of internet: prospects, trends, and challenges," Cluster Computing, 2021.
[25] B. Le Nguyen, E. L. Lydia, M. Elhoseny, et al., "Privacy preserving blockchain technique to achieve secure and reliable sharing of IoT data," Sensors, Materials & Continua, 2020.
[26] C. Stolojescu-Crisan, C. Crisan, and B. P. Butunoi, "An IoT-based smart home automation system," Sensors, 2021.
[27] L. Da Xu, Y. Lu, and L. Li, "Embedding blockchain technology into IoT for security: A survey," IEEE Internet of Things Journal, 2021.
[28] A. Al Sadawi, M. S. Hassan, and M. Ndiaye, "A survey on the integration of blockchain with IoT to enhance performance and eliminate challenges," IEEE Access, 2021.
[29] A. N. Bikos and S. A. P. Kumar, "Securing digital ledger technologies-enabled IoT devices: taxonomy, challenges, and solutions," IEEE Access, 2022.
[30] M. Shurman, A. A. R. Obeidat, et al., "Blockchain and smart contract for IoT," in Proc. 11th International Conference on Information and Communication Systems (ICICS), pp. [insert page numbers], 2020.
[31] H. M. Verhelst, A. W. Stannat, and G. Mecacci, "Machine learning against terrorism: how big data collection and analysis influences the privacy-security dilemma," Science and Engineering Ethics, 2020.
[32] L. Gong, D. M. Alghazzawi, and L. Cheng, "BCoT sentry: A blockchain-based identity authentication framework for IoT devices," Information, 2021.
[33] H. F. Atlam, M. A. Azad, A. G. Alzahrani, and G. Wills, "A Review of Blockchain in Internet of Things and AI," Big Data and Cognitive Computing, vol. 2020.
[34] P. Bellavista, C. Esposito, L. Foschini, C. Giannelli, et al., "Interoperable blockchains for highly-integrated supply chains in collaborative manufacturing," Sensors, 2021.
[35] S. Jabbar, H. Lloyd, M. Hammoudeh, B. Adebisi, et al., "Blockchain-enabled supply chain: analysis, challenges, and future directions," Multimedia Systems, Springer, 2021.
[36] W. Ou, S. Huang, J. Zheng, Q. Zhang, et al., "An overview on cross-chain: Mechanism, platforms, challenges and advances," Computer Networks, 2022.
[37] H. Touqeer, S. Zaman, R. Amin, M. Hussain, F. Al-Turjman, and M. Bilal, "Smart home security: challenges, issues and solutions at different IoT layers," The Journal of Supercomputing, vol. 77, no. 12, pp. 14053-14089, 2021.
[38] S. G. Andrae, "New perspectives on internet electricity use in 2030," Engineering and Applied Science Letter, 2020.
[39] H. Honar Pajooh, M. Rashid, F. Alam, and S. Demidenko, "Multi-layer blockchain-based security architecture for internet of things," Sensors, 2021.
[40] M. Kalinin, D. Zegzhda, and E. Zavadskii, "Protection of energy network infrastructures applying a dynamic topology virtualization," Energies, 2022.
[41] K. H. Kang, M. S. Kim, J. J. Kim, and Y. In, "Risk Factors and Preventive Strategies for Perioperative Distal Femoral Fracture in Patients Undergoing Total Knee Arthroplasty," Medicina, 2023.
[42] Z. Rahman, X. Yi, I. Khalil, and A. Kelarev, "Blockchain for IoT: A Critical Analysis Concerning Performance and Scalability," 2021.
[43] B. M. Agostinho, M. A. R. Dantas, and A. S. Roschildt Pinto, "Proposal of an Economy of Things Architecture and an Approach Comparing Cryptocurrencies," 2021.
[44] H. D. Zubaydi, P. Varga, and S. Molnár, "Leveraging Blockchain Technology for Ensuring Security and Privacy Aspects in Internet of Things: A Systematic Literature Review," 2023.
[45] M. Ansari, S. A. Ali, and M. Alam, "A Synergistic Approach for Internet of Things and Cloud Integration: Current Research and Future Direction," 2019.
[46] N. Azizi, H. Malekzadeh, P. Akhavan, O. Haass, et al., "IoT–Blockchain: Harnessing the Power of Internet of Thing and Blockchain for Smart Supply Chain," 2021.
[47] M. M. Akhtar, D. R. Rizvi, M. A. Ahad, S. S. Kanhere, et al., "Efficient Data Communication Using Distributed Ledger Technology and IOTA-Enabled Internet of Things for a Future Machine-to-Machine Economy," 2021.
[48] L. Hang and D. H. Kim, "Design and Implementation of an Integrated IoT Blockchain Platform for Sensing Data Integrity," 2019.
[49] S. K. Singh and S. Kumar, "Blockchain Technology: Introduction, Integration and Security Issues with IoT," 2021.
[50] C. H. Wu, Y. P. Tsang, C. Ka-Man Lee, and W. K. Ching, "A Blockchain-IoT Platform for the Smart Pallet Pooling Management," 2021.
[51] M. R. Alagheband and A. Mashatan, "Advanced encryption schemes in multi-tier heterogeneous internet of things: taxonomy, capabilities, and objectives," 2022.
[52] J. A. Guerra, J. I. Guerrero, S. García, S. Domínguez-Cid, et al., "Design and Evaluation of a Heterogeneous Lightweight Blockchain-Based Marketplace," 2022.
[53] M. Maroufi, R. Abdolee, and B. M. Tazekand, "On the Convergence of Blockchain and Internet of Things (IoT) Technologies," 2019.
[54] Xie, Q. Zhang, and J. Qin, "Joint Optimization of Cooperative Communication and Computation in Two-Way Relay MEC Systems," 2019.

[55] A. K. Tyagi, S. Dananjayan, D. Agarwal, and H. F. T. Ahmed, "Blockchain—Internet of Things Applications: Opportunities and Challenges for Industry 4.0 and Society 5.0," 2023.

[56] A. Alkhateeb, C. Catal, G. Kar, and A. Mishra, "Hybrid Blockchain Platforms for the Internet of Things (IoT): A Systematic Literature Review," 2022.

[57] R. Zhang, C. Xu, and M. Xie, "Secure Decentralized IoT Service Platform using Consortium Blockchain," 2022.

[58] Rai, H. M., Shukla, K. K., Tightiz, L., & Padmanaban, S. (2024). Enhancing data security and privacy in energy applications: Integrating IoT and blockchain technologies. *Heliyon*, *10*(19).

[59] Kumar, P., Kumar, R., Aljuhani, A., Javeed, D., Jolfaei, A., & Islam, A. N. (2023). Digital twin-driven SDN for smart grid: A deep learning integrated blockchain for cybersecurity. *Solar Energy*, *263*, 111921.

[60] Cornel-Cristian, A., Gabriel, T., Arhip-Calin, M., & Zamfirescu, A. (2019, September). Smart home automation with MQTT. In *2019 54th International Universities Power Engineering Conference (UPEC)* (pp. 1-5). IEEE.

[61] Kurdi, H., & Thayananthan, V. (2022). A multi-tier MQTT architecture with multiple brokers based on fog computing for securing industrial IoT. *Applied Sciences*, *12*(14), 7173.

[62] Hazzaa, F., Hasan, M. M., Qashou, A., & Yousef, S. (2024). A New Lightweight Cryptosystem for IoT in Smart City Environments. Mesopotamian Journal of CyberSecurity, 4(3), 46–58.

[63] Mijwil, M., Ruchi Doshi, Kamal Kant Hiran, Abdel-Hameed Al-Mistarehi, & Murat Gök. (2022). Cybersecurity Challenges in Smart Cities: An Overview and Future Prospects. Mesopotamian Journal of CyberSecurity,2022,1–4.

[64] Plageras, A. P., Psannis, K. E., Stergiou, C., Wang, H., & Gupta, B. B. (2018). Efficient IoT-based sensor BIG Data collection–processing and analysis in smart buildings. *Future Generation Computer Systems*, *82*, 349-357.

[65] Zaidi, S., Bitam, S., & Mellouk, A. (2017, May). Enhanced user datagram protocol for video streaming in VANET. In *2017 IEEE International Conference on Communications (ICC)* (pp. 1-6). IEEE.

[66] Gaur, A., Scotney, B., Parr, G., & McClean, S. (2015). Smart city architecture and its applications based on IoT. *Procedia computer science*, *52*, 1089-1094.

[67] A. Alsajri, A. Steiti, and H. A. Salman , Trans., “Enhancing IoT Security to Leveraging ML for DDoS Attack Prevention in Distributed Network Routing”, BJIoT, vol. 2023, pp. 74–84, Oct. 2023, doi: 10.58496/BJIoT/2023/010.

[68] L. Hussain, “Fortifying AI Against Cyber Threats Advancing Resilient Systems to Combat Adversarial Attacks”, EDRAAK, vol. 2024, pp. 26–31, Mar. 2024, doi: 10.70470/EDRAAK/2024/004.