National College of Ireland

Decentralised Based SDP for IoT Ecosystem in Edge Computing

MSc Research Project

Msc in Cloud Computing

Prabhav Gaur

Student ID: x22245316

School of Computing

National College of Ireland

Supervisor:Sudarshan Deshmukh

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Prabhav Gaur……
Student ID:	……x22245316……..……
Programme:	Msc in Cloud Computing **Year:** 2023 -2024
Module:	……Research Project (MSCCLOUD1_B)…….……
Supervisor:	……Sudarshan Deshmukh…….……
Submission Due Date:	……12/08/2024…….……
Project Title:	Decentralized Based SDP for IoT Ecosystem in Edge Computing
Word Count:	……7855…… **Page Count**……20……..……..

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: ……Prabhav Gaur……

Date: ……12/08/2024……

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Decentralised Based SDP for IoT Ecosystem in Edge Computing

Prabhav gaur

x22245316

Abstract

The rapid expansion of the Internet of Things (IoT) and its integration with edge computing has revolutionized data collection, sharing, and analysis across various domains, including smart homes, healthcare, industrial automation, and smart cities. However, this growth has introduced significant security challenges due to the decentralized and dynamic nature of IoT networks.Centralized traditional security models that are based on controlling access and defining clear perimeters of a networked organism are insufficient to protect these environments. This paper proposes a SDP architecture that breaks down the barriers of centralized implementation by built and simulated on the blockchain concept. This paper integrates the SDP which helps in dynamic policy enforcement and fine-grained access control with blockchain, which provides decentralization, immutability, and transactional transparency in implementing security provisions for IoT networks. In this study, simulation reveals the applicability of the framework on establishing secure device interactions, conducting edge and fog computations, and documenting all activities and communications in a transparent and tamper-proof manner. The practical implementation brings out the idea that the framework undergoes constant adjustment with the network changes in an effort to utilize the mechanisms in the continual protection of networks without the experience of degraded performance. These findings present a solid foundation for further development of security, scalability and reliability of IoT environments, which should offer further possibilities for the application and utilization of IoT systems in different applications.

Keywords :

IoT Security, Edge Computing, Software-Defined Perimeter, Blockchain Technology, Decentralised Security, Real-Time Monitoring, Scalability, Dynamic Policy Enforcement, Fine-Grained Access Control, Immutable Ledger.

1. Introduction

1.1 Background on the Research Topic

The Internet of Things (IoT) has fundamentally transformed the landscape of contemporary technology with the inter-connective web of the devices currently in the market. . This paradigm Shift has currently influenced areas such as the smart homes, smart health, industrial applications, smart city hence causing a massive production of data.

For example, the thermostats, the lights and the security systems of smart homes are integrated smart devices that work together to improve the convenience, safety, and energy saving of homes. Smart cities employ IoT for resource management, traffic control and optimization of the lives of people in urban areas. To deal with the large amount of data which is being produced by such IoT applications, a critical innovation called edge computing has arisen. Edge computing means supported computing and storage closer to the source of data and not dependent on the data which is sent to central cloud servers.

This eliminates distance-related latency hence the opportunity of faster and real-time computation of data. For instance, in self-driving cars, decisions regarding the avoidance of an accident have to be made in millions of microseconds due to the critical calculations involved; hence, the data has to be processed at the edge. Edge computing also reduces bandwidth consumption as it gathers the information to be sent to the cloud and only sends that information instead of constantly sending raw data, especially in those with restricted bandwidth or very fast data generation.

1.2 Justification for the Research

However, it is important to note that IoT networks are distributed and decentralized, and this comes with a lot of security vulnerabilities. Unlike classic centralized systems where the security policies are relatively easy to enforce within the well-known perimeter, IoT solutions consist of many different loosely interconnected devices. These devices differ in their computational power, operating systems or unification, and the level of security. To illustrate this, the security characteristics may vary, depending on what device is in question: whether a smart thermostat, an industrial robot, or a medical sensor. It becomes challenging for all the organizations within the network to apply the same security standards since they differ in their needs, size, locations, and other organizational characteristics.

IoT networks are distinguished by their dynamic topology. Data holders frequently attach and disconnect to the network, roam around, and communicate with other devices and data holders capriciously. This dynamism contributes to the growth of the attack surface since it is difficult to identify and prevent security threats. Few challenges associated with the IoT are security threats which include intrusion, data theft, and cyber threats such as DDoS attacks. Eternal access is a situation in which an attacker assumes command and control of a device or obtains data under his control. When such occurrences happen, personnel or clients' information might end up in the wrong hands thus posing a serious threat. Based on the data received, potential threats and risks of cyber attacks may affect the functioning of IoT networks, thus causing service interruptions, material losses, and physical damage.

1.3 Research Gap

The problem of traditional security is rather evident with current IoT systems, which overall lack formal, global control points and ultimately rigid boundaries when it comes to security. Old-fashioned solutions do not offer sufficient levels of protection when the devices are diverse, often portable, and are in constant dynamic communion. These challenges are even aggravated by the fact that large volumes of data need to be processed in real-time while often in environments with limited resources as is the case with edge computing.

This research presents an innovative new decentralized implementation of Software-Defined Perimeter (SDP) architecture which is accompanied by smart contract based on blockchain ethereum network. While my proposed framework aimed at ending on the basic problems of security and scalability in IoT systems running in edge computing territories.

The strength of this concept is based on the integration of the dynamic policy enforcement and the per-subject access control mechanisms in SDP with the reliability of the distributed ledger from the blockchain platform. Through the integration of these technologies, the given framework provides a large-scale solution which is also quite scalable and adaptable to demands that are required for IoT networks in future.

1.4 Research question and Hypotheses

What are the potential benefits of integrating Software-Defined Perimeter (SDP) architecture with blockchain-based smart contracts in enhancing IoT security?

The integration of SDP architecture with blockchain-based smart contracts can significantly improve the security and scalability of IoT networks.

1.5 Document structure

The structure of the research paper is designed to provide exhaustively the integration of Software-Defined Perimeter (SDP) architecture with blockchain for IoT security improvement. The purpose and scope of the study are defined in the Introduction Section where the context for the particular work is provided, existing traditional security models documented, research problem and questions identified, and the hypotheses are formulated. In the Literature Review we discuss modern approaches to IoT security and reveal the shortcomings of existing solutions in the field of constantly developing threat vectors. The Methodology describes the concept of the decentralized SDP together with the simulation environment, smart contract design, and hierarchy of data processing. The Results section contains information on how the framework is effective for raising security, scalability and adaptability to different conditions. The Discussion of these findings contrasts the methods into the framework and the practicality of its potential application. Last but not least, the Conclusion revisits the research findings and directions for future work, including the enhancement of the effectiveness of blockchain protocols and investigations of new technologies to be integrated into the system.

2. Related Work

The integration of IoT with the concept of edge computing has brought immense changes in the current generation of real-time data processing and decision making in niches such as smart city, health care, and industrial applications. However, this integration has come with new forms of cybersecurity threats especially due to the IoT systems that are complex and heterogeneous in nature. Specifically, the known traditional security models that focus on the concept of control and perimeter protection are insufficient to define the new computational environment of IoT networks.

2.1 Emerging Security Challenges

2.1.1 Cybersecurity Challenges in Edge Computing and IoT

IoT in connection with edge computing brings new security issues into view; first, these are related to the decentralised and heterogeneous structure of such networks. Al-Rakhami et al mention the threats of edge computing including the threats of data theft and apprehending privacy in edge computing

environment. They recommend that incorporating blockchain as a technology can reduce such risks through decentralising the platform use in data management and communication.
Almuseelem also describes these challenges in the framework of Healthcare 4. Often equal to zero, because the protection of pharmaceutical data is a matter of concerns due to their nature that is strongly connected with the healthcare field. The proposed ZTA-based framework has been targeting to counter all the numerous cyber threats through constantly identifying and authenticating all the connected devices and also guaranteeing end-to-end secure data communication throughout the network.

Massive Numbers of Vulnerable IoT Devices: Such devices typically have low computational power, for which they can have poor security measures, for example, point forging and/or denial of service (DoS).
Data Privacy and Security: It is challenging to maintain figures' privacy at the edge nodes where data is processed, and consequently, it is necessary to implement multiple layers of security..
Trust and Trustworthiness: Inter-device and IoT device with edge platform trust needs to be built. Building recurrent and efficient trust management strategies constitutes another research implication

2.1.2 Decentralized Security Management

Centralized security models do not work well for the IoT networks because it lacks decentralized architecture. Due to the dynamicism of devices and connections, the network environment has an unceasingly shifting perimeters and thus the layered perimeter security cannot be efficient here. Decentralized security management with the help of technologic instruments like blockchain implies the distribution of security functions throughout the net and decreases the opportunities for adversaries to attack the concentrative aspects of networks. In their paper on the analysis of threats to edge computing, Pan and Yang (2018) state that "due to this new face of Internet that is currently shifting from a centralised one to the Internet of Things (IoT), centralised data models cannot prevails". The authors lay their emphasis on the decentralized approaches stressing on the fact that the existing approaches for large volumes and velocity of data generated by IoT devices are inadequate. Ragothaman et al. (2023) further strengthen this by explaining the perennial review difficulty of access control in IoT because of the distributed frame of these systems. They continue and indicate that "IoT networks encompass devices with different hardware and software characteristics and, thus, the heterogeneity of IoT environment presents significant challenges for the access control solution. "

Almuseelem in his paper says that, Zero-Trust Architecture (ZTA) is very effective for the decentralized security management in Healthcare 4. 0. ZTA operates under the assumption that every entity that is within the network is hostile, meaning that there has to be constant authentication, and dynamic policy enforcement with relation to; Device to Device (D2D), Device to Edge (D2E), and Edge to Cloud (E2C).

2.1.3 Scalability and Flexibility

Edge computing is said to make scaling possible by handling data processing locally and Pan and Yang (2018) explain this as the ability to: minimise data communication especially in the backbone internet, derive in-situ data insights, increase the response rate and decrease the response time. At the same time, with this approach, not only is scalability improved, but flexibility in relation to data processing and interaction with this data is also added, since the edge devices build exactly the necessary reactions, and do not overload the cloud.
As stated by Al-Rakhami et al., the use of edge computing with blockchain enhances scalability because computational operations and data storage are distributed among multiple nodes. The given distributed structure improves the network's scalability without negatively influencing the efficiency.

2.2 Existing Security Models and Their Limitations

2.2.1 Decentralised Blockchain-Based Models

Albshri et al describe more on how blockchain technology may be used to overcome current IoT centrally deigned architectures. The node to node model authorized by the blockchain space presented the decentralized best practice that diminished the single points of failure that are typical to IoT centrality schemes. These make the distribution of files enhanced and improves on the fault tolerance since there is no centering of the servers. Blockchain's decentralized data storage, as well as its immutability, also improves the security and integrity of IoT systems and is an ideal solution for decentralised IoT networks. The realisation of these systems requires efficient simulation tools for assessing the real-world effectiveness of such systems with stress on the combination of blockchain and IoT.

2.2.2 Conceptual Models and Simulation

Albshri et al. further to the above proposals by presenting a conceptual architecture for the simulation of blockchain-based IoT environments. This model proposes a concept of a realistic simulation framework which can assess and validate the blockchain based IoT application concerning the issues of scalability, security and reliability. Some of the proposed features and capabilities can be summarized in the following main areas of the overall architecture: It is considered critical for potential problems and fine-tuning of the system before its implementation to stress the significance of simulating decentralized blockchain-based IoT models.

2.2.3 Hierarchical Security Paradigms

The peculiarities of IoT and edge computing create security issues that are hard to handle, and to address these problems, there is a concept of hierarchical security paradigms. Pan and Yang are among the authors who have addressed the problematic of possibility to integrate hierarchical models with edge computing to build the multiple-layered security, that will raise data intelligence at the place of data production, decreased latency issues and increased response speed as well as provide higher security.
This layered security approach is further complemented by the work of Ragothaman et al. (2023) in which the authors have underscore the fact that the access control solutions that must be inherently multi-layered to operate in the context of the IoTs network.

According to them, hierarchical security models are effective in dealing with the IoT system complexity since they offer a tiered security mechanism in device, network, and application layers. This makes certain that the measures of security that are being implemented are balanced as well as relevant depending on the layer that has been implemented.

2,2.4 Software-Defined Security (SDS)

Software-Defined Security (SDS) is turning out to be the most suitable approach of securing dynamic and complicated IoT networks. In the paper SDS is incorporated within a ZTA framework to describe how security policies can be changed dynamically based on threat intelligence gathered in real time as deem by Almuseelem. This makes it possible for the system to be flexible so as to cater for the security of the network as it continually change due to the emerging threats.

Paper Title	Methodology	Research Domain	Achievements	Limitations	Differentiation

Decentralised Blockchain-Based Model for Edge Computing	Development and simulation of a decentralized model integrating blockchain with edge computing.	Integration of Blockchain and edge computing technologies	efficient access to networks by numerous devices	Challenges in addressing privacy and security concerns due to outsourced services supporting operations at the edge of networks	Integrates blockchain to enhance security in edge computing, whereas my paper specifically focuses on SDP for IoT in edge computing using blockchain for dynamic policy enforcement.
Cybersecurity Challenges and Opportunities in the New "Edge Computing + IoT" World	Analysis of emerging cybersecurity challenges and opportunities in edge computing and IoT.	Cybersecurity in Edge Computing and IoT	Identifies key challenges and highlights opportunities involving AI, blockchain, and lightweight security.	Theoretical approach, lacks empirical validation or implementation.	Primarily theoretical, focuses on identifying challenges and opportunities without proposing a concrete, implementable framework like the SDP in my paper.
Decentralized Task Offloading in Edge Computing: A Multi-User Multi-Armed Bandit Approach	Design and simulation of a decentralized multi-user task offloading scheme using a multi-armed bandit approach.	Edge Computing and Task Offloading	Achieves near-optimal task offloading performance with sub-linear regret in dynamic and uncertain environments.	Challenges in achieving a fair edge resource allocation and respect for capacity limits to avoid service blockage	Focuses on decentralized task offloading using online learning, contrasting with my paper's blockchain-based security framework for IoT in edge computing.
Hierarchical Security Paradigm for IoT Multiaccess Edge Computing	Proposal of a software-defined perimeter (SDP) framework to supplement MEC and provide added security	Security challenges in MEC such as location-based attacks, man-in-the-middle attacks, and sniffing, addressed by SDP	Implementation of SDP within a mobile-edge LTE network and demonstration of its resilience to DoS attacks	SDP faces challenges like trust management and authentication issues that can lead to various attacks	Focuses on combining SDP with MEC for hierarchical security, differing from my paper's decentralized blockchain-based SDP framework for IoT in edge computing.
Toward a Secure 5G-Enabled Internet of Things: A Survey on Requirements, Privacy, Security, Challenges, and Opportunities	Investigation of benefits and issues of 5G-enabled IoT, including privacy and security concerns and technology enablers	Securing 5G-enabled IoT infrastructure with billions of connected devices, focusing on privacy and security enhancements	Enhancements in reliability, practicability, efficiency, and user experience by incorporating 5G technology into IoT	Need for interdisciplinary research to address the research obstacles and security concerns for 5G-enabled IoT	Provides a broad survey of 5G-IoT challenges and opportunities, unlike my paper's specific focus on a decentralized blockchain-based SDP framework for IoT security.
Enabling Zero-Trust	Proposal and simulation of a	Cloud-Edge Computing	Enhances security and	Primarily simulation-based;	Focuses on Zero-Trust principles and continuous

Architecture-Based Security Framework for Cloud-Edge Computing-Based Healthcare 4.0	Zero-Trust Architecture with continuous lightweight mutual authentication for healthcare environments.	Security in Healthcare 4.0	privacy in healthcare systems through continuous authentication and identity-based access control.	lacks real-world validation and might incur computational overhead in resource-constrained environments.	mutual authentication specifically for healthcare, contrasting with your paper's broader application of blockchain-based SDP for IoT in edge computing.
Edge of Things Inspired Robust Intrusion Detection Framework for Scalable and Decentralized Applications)	Design and simulation of a multilayered EoT framework with machine learning-based intrusion detection.	IoT, Edge Computing, and Security.	Improved intrusion detection, response rate, and scalability in decentralized applications.	Not tested in real-world scenarios	Focuses on enhancing intrusion detection in decentralized EoT environments, offering a layered approach, unlike the blockchain-based security framework in my paper.
A Conceptual Architecture for Simulating Blockchain-Based IoT Ecosystems	Conceptual architecture for blockchain-based IoT	Blockchain, IoT	Framework for simulating blockchain-based IoT applications	Lack of large-scale environment tests	blockchain-based SDP framework for IoT security.
Access Control for IoT: A Survey of Existing Research, Dynamic Policies and Future Directions	Survey on access control in IoT	Access Control, IoT	Comprehensive survey on IoT access control mechanisms	Challenges in dynamic policy specification	Focuses on surveying existing research and future directions for access control in IoT, whereas my paper proposes a simulation based research onl decentralized SDP framework for IoT security in edge computing environments.
An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via Software-Defined Security	Comprehensive review and proposal of SDN-based security frameworks for IoT systems.	IoT Security with Software-Defined Networking (SDN)	Thorough analysis of IoT security challenges and introduction of SDN-based countermeasures.	Theoretical framework with limited real-world implementation or empirical validation.	Focuses on using SDN to provide a network-based security approach for IoT, unlike the decentralized blockchain-based approach in my paper.

(Table 1).

Conclusion and Insights for Implementation

Summary of Key Insights

The paper shows that there have been remarkable progress and still emerging issues concerning IoT and edge computing security namely decentralized models. Centralized security models are rather ineffective in the contemporary IoT context because these environments are costly in terms of flexibility and heterogeneity. In his review, he discusses how decentralized security management, for example with the help of blockchain has the possibility to overcome these shortcomings. Distributed características of blockchain provide better tolerance for failure and overall cost savings, as well as the ability to protect data from modification, which can make it a suitable technology for IoT systems. Furthermore, when it comes to the Software-Defined Security (SDS) frameworks, especially when implemented under Zero-Trust Architectures (ZTA), there is flexibility in security measures that make them respond to actual threats, thus improving IoT's systems' security.

There is a growing necessity for the hierarchical security paradigms to handle the complexity of the IoT and the edge computing. These models also incorporate a layer by layer approach of security at device level, security at network level and application level security in other words, the security mechanisms used in these models are pertinent and appropriate at each tier. This layered approach used in combination of the decentralized model such as the blockchain could help in the enhancement of security as well as scalability of IoT networks.

3. Research Methodology

3.1 Proposed Framework: Decentralised SDP By Smart contract

Because of the increasing complexity and distribution of IoT-based systems catalyzed by the impact of the distribution of compute loads and shift to edge computing, mashing and highly scalable security cannot be overemphasized. To address these issues, this study proposes a distributed version of an SDP solution integrated with a blockchain. This paper describes the building of the anticipated framework that should provide resilient, flexible, and retractable security to IoT systems, coupled with data, access, and real-time threat protection. Conceptual Framework: The development of the suggested framework started from the definition of the main issues with protecting IoT environments, particularly those based on the edge computing concept. There also exist original security models that are not sufficient since IoT networks are developing and rather decentralized. To counteract these problems, this conceptual framework was developed with an aim to integrate the blockchain solution by smart contracts due to their efficiency in establishing a decentralized, therefore secure and transparent environment. Thus the framework was designed to enable dynamic policy enactment, high-level access control, as well as logging all interactions with devices.
These features are instrumental in making IoT systems secure and as the IoT systems grow or extend the features mentioned are important for their security.

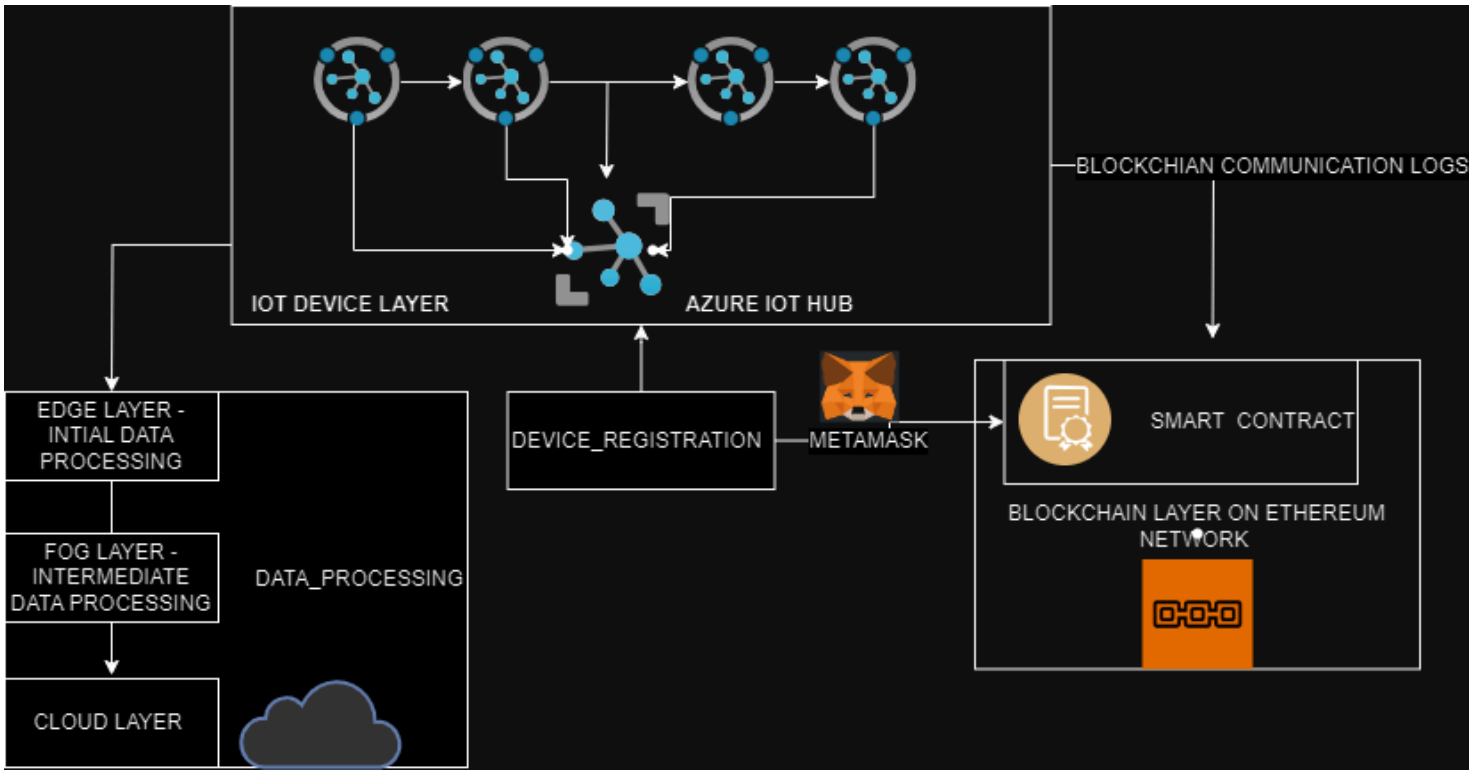
3.1.1 Fine-Grained Access Control

The simulation which was incorporated in the blockchain system included the registration and authentication of IoT devices. Every device was provided with an identification number and two cryptosignals for the purpose of identification. The registration process ensured that only the genuine devices were to be allowed to be a part of the network, thus ensuring that the threats from various hacker attacks were minimized.

3.1.2 Immutable Blockchain Ledger

Tamper-Proof Record Keeping: This is because the applications of blockchain technology employ a distributed ledger which cannot be edited restricting the alteration or deleting of documentation of a certain transaction or an interaction. Each transaction is encrypted and can be checked by the several nodes of the network increasing the level of its security. It remains constant to provide a reliable record of all the activities performed within the IoT network.

Distributed Validation: In the case of blockchain, the ledger is distributed and held at several locations involving all nodes that get to validate transactions by consensus. This is important as it eliminates the risk of having a single failure point and the ledger's continuity is maintained even by corrupted nodes. In regard to IoT, this is to say that all the other products in the network will still be secure even when the other products are under an attack.



(Architecture diagram)Figure 1

3.2 Methodology Justification

The simulation results provided strong validation of the research question: “If and how a decentralized SDP framework will provide an overall improvement in security and scalability for IoT deployed in edge computing?” In fact, the success of the actual IoT devices’ communication was 88.89%. Actually, the effectiveness of the proposed decentralized software defined perimeter plan involving blockchain technology is proved by the 100% successful rates of registered device’s authentication. This framework effectively responded to the fundamental issues of IoT security and scalability as it allowed only the legitimate devices to engage in the network, and as the communication between manifold kinds of devices was properly organized.

3.2.1 Validation of Security Enhancements:

The inclusiveness of the framework, which offered a total rejection of all devices not previously registered on the framework, can be seen as a primary strength and proof of the security of the system in its efficacy in the rejection of unregistered items, with a 0 % success rate indicated for all such items. Many current models of IoT imply the utilization of static and less protective measures, thus making them susceptible to hacking and other unauthorized activities. On the contrary, the proposed decentralized SDP framework incorporates the distributed ledger and the dynamic access control which makes them more secure than conventional frameworks. This way, every device involved in the execution of the procedure goes through a strict authentication check before it can indulge into communication, minimizing the risk of the penetration by abusers and boosting the security levels of the IoT context.

The stability and reliable performance of the registered devices in the different scenarios of communication also supports the fact that the proposed framework addresses the management of dynamics and decentralization in the present complex IoT contexts. In terms of information protection, the framework shows that it possesses the ability of excluding unauthorized users’ access to IoT messages, and securely recording and storing all the communications on the blockchain.

3.3 Application of Methodology

3.3.1 Enhanced Security in IoT Ecosystems:

Thus, the results of the simulation present a high concern regarding the security of IoT ecosystems. The specified interaction framework with the utilization of blockchain for the record of all the interactions between devices is actually the way to build trustful and secure IoT systems required in present days. Thus, the proposed framework makes all the transmitted data and communication well-protected and prevents dangerous intrusions which threaten the common and known IoT systems.Also, the dynamic nature of SDP framework makes it possible to consider the changes that occur in the network as well as in the device and apply the necessary changes promptly. This capability is useful in IoT networks where the nodes continuously associate, disassociate, or roam within the network. This aspect of the framework is very effective since it enables the updates of the security policies within the framework that is within the network to counter threats that may develop within the ecosystem. This dynamic adaptability is a huge leap from static security schemes which are deemed too rigid for decentralised IoT networks’ ever-shifting nature and structure.

4. Design Specification

4.1 Environment Setup:

A simulation framework for comprehensive device simulation was built with Python, and Web3 for blockchain interface and Azure IoT SDK for device interfacing. To ensure the aspects of reality and the use of various devices with different roles and communication patterns are taken into account the simulation environment was developed with the following elements: This arrangement provided the Medium for the testing and validation of the framework under real-world like IoT deployment scenarios.

4.2 Implementation of Smart Contracts:

Smart contracts were overseeing the registration of the device, the authentication and the logging communications. The smart contracts which were used in the design was programmed to implement Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) that would adapt to the changing state of the environment. This strategy makes it possible to always have a proper correlation between access control decisions and the existing state of security of the network and thus reduce the chances of intrusion.The smart contracts also contained the capability to record all communication between devices, and the resulting information was saved chronologically on the blockchain; this record could be reviewed for safety and compliance checks. This type of logging is very essential in security since it focuses on real-time activities in the network by creating a transparent log file that cannot be tampered with.

4.3 Integration with Azure IoT Hub:

To apply the decentralized SDP framework to actual IoT environment, the framework is also interfaced with the Azure IoT Hub. For handling the IoT devices and its interaction with the cloud services, Azure IoT Hub was chosen since it offers very good functionalities and is reliable. The IoT Hub became the control center of the device interconnection, data acquisition, and computing in the network. This integration enabled the framework to accommodate a vast array of devices, including the traffic light, environmental sensors, smart meter, and security camera, with the framework's security as well as scalability.The integration with Azure IoT Hub also allowed the framework to offload certain computational intensive and storage tasks to the cloud while making sure that certain user data processes occurred closer to the source of the data at the edge. In addition to that, this approach helped scale the framework and also drastically helped in decreasing the latency and thus it was suited for large scale IoT.

4.4 Strengths and Limitations of the Approach

The simulation results exhibit relatively high potential for the targeted approaches, though there are still difficulties and further research topics to address. While it improves the framework's security and transparency with the help of blockchain technology, this may result in certain challenges related to transaction speeds and energy requirements, in particular when integrated on a larger scale. Future studies could draw the analysis of how to have better solutions to the mentioned challenges by incorporating the efficient consensus algorithms or the integration of blockchain with other technologies.

Furthermore, the simulation proved the ability of the framework in scaling up and handling more devices, however, more experimentation with more devices and varying topologies is needed to assess

the highest level of performance of the framework in practical settings. To identify further opportunities and possible limitations of the framework's application, it will also be helpful to examine its relevance for a broad range of IoT applications and contexts.

The proposed decentralized SDP framework coupled with blockchain is more novel in providing enhanced security and scalable IoT infrastructure. The above simulation results confirm that the proposed framework is a feasible solution for the mentioned issues of IoT security and system scalabilities and hence can be implemented across various fields. The proposed framework offers improved security by providing rigorous authentication measures and tamper-proof recording, as well as increased scalability by extending the distributed IoT architecture to integrate hierarchal computing; therefore, it has the potential to become the future of IoT networks. In the future of IoT advancements, such frameworks will always be useful in the IoT role of providing security, scalability and efficiency in deploying IoT technologies to different complex networks.

5. Implementation

The efficiency of the decentralized SDP framework incorporating blockchain, a comprehensive simulation was performed. This simulation was set in a manner that closely resembled an actual IoT environment and was used to test the efficiency of the framework in managing and securing the complicated and dispersed IoT system. The scenario was intended to be very close to real-world IoT projects and hence it incorporated multiple aspects of IoT, including a variety of devices, dynamic networks and the requirement of growth of security solutions.

5.1 Simulation Environment

This simulation environment was deliberately built to replicate the actual IoT environment similar to smart cities, industry 4.0, and smart homes. The environment included various types of devices, each playing a specific role in testing the framework's capabilities:The environment included various types of devices, each playing a specific role in testing the framework's capabilities:

- Important components of the infrastructure were approximated with Traffic Lights so that they could operate securely and dependably.
- Environmental Sensors track things like air and surface temperature, whereby the integrity of the data transfer along with analysis was important.
- Smart Meters expressed the energy consumption by the user, which required a more secure way of data acquisition and a strict policy on the protection of the data.
- Security Cameras offered surveillance and the feeds' integrity as well as confidentiality were a priority.
- Smart Home Appliances were things such as thermostats and smart locks and these had to have a secure method of communication to avoid malicious Parties controlling them.

Each device in this simulated environment was registered and authenticated using the blockchain-based decentralised SDP smart contract, ensuring consistent application of the security protocols.

5.2 Device Registration and Authentication

The first process of the simulation involved the every IoT device registered and authenticated, a crucial procedure to develop a reliable and trustworthy network. The process involved:

- **Cryptographic Key Generation:** Each device generated a unique cryptographic key pair, consisting of a public key for identification on the blockchain and a private key for signing transactions and authenticating the device.
- **Blockchain Registration:** The device's public key, credentials, and permissions were recorded on the blockchain, creating a permanent and immutable record of the device's identity and authorized capabilities within the network.
- **Authentication Process:** Before a device could interact with other devices or access network resources, it authenticated itself using its cryptographic keys. The blockchain verified the device's identity and checked its permissions against the recorded data, ensuring that only authenticated devices could join the network.

This process made sure that all the devices in the network are authorized and trusted hence minimizing a lot of unauthorized entry into the network and other malice acts.

5.3 Edge and Fog Layer Data Processing

Due to the large volume of data produced by the IoT devices, the simulation based on the system simulate a two-tiered structure, namely the Edge and the Fog computing layers. This approach shows how the network take care of the latency problem as well as the usage of the bandwidth and adequacy of time in handling data.

- **Edge Layer Processing:** Real-time data processing in near real-time applications closer to the data origination was performed at the edge. For instance, data were generated from traffic lights and environment sensors, where the resulting information must be immediately acted upon, for instance changing the color of the traffic lights depending on environmental conditions. Acquiring and processing such data at the edge reduced decision opportunities' lateness and the data transmission back to a central node.
- **Fog Layer Processing:** A fog layer existed in between an edge device and the cloud and was able to perform slightly intricate and demanding operations mainly related to data analysis. The fog layer dealt with functions that demanded more computational capacity than the edge could offer, for example, processing data collected from smart meters to determine energy usage or identifying irregularities in security cameras' footage.

Through a hierarchical model, the data would be processed optimally and with maximum security, with initial actions on the edge layer while further analysis would be on the fog layer.

5.4 Blockchain Logging of Communications

One of the most important aspects of the developed simulation was the possibility of storing all inter-device communication records in a blockchain. The stated mechanism was helpful to provide the curtain of transparency and impenetrable ledger of all transactions that took place in the network, therefore removing the chances of unaccountability or enablement of any deceitful actions.

- **Recording Interactions:**Any communication between devices was made on the blockchain with more fields; sender ID, receiver ID, message, time stamp included. This information was then recorded into the blockchain technology, which ensures that the data cannot be edited, deleted or manipulated in any way hence acts as a record in the audit trail.
- **Transparency and Accountability:** The fact that it was a block chain system meant that once a particular communication had been recorded in the block, then it could not be erased or changed. This openness was useful to justify the honesty of all the stakeholders and was used to check for any compelling actions from the network.
- **Anomaly Detection and Auditing:** The logs also had a great significance in identifying the inefficiencies or an anomaly of the system. An analysis of that logged data could subsequently reveal certain levels of communication that would be deemed suspicious for any security breaches, for example, unauthorized access or corrupt devices. The provision for auditing these logs offered another level of security, where the logs could be scrutinized in the aftermath of an incident and the organization's security system could be improved.

5.5 Key Findings from the Simulation

The simulation generated several important conclusions that proved the efficiency of the proposed framework when it comes to security and building of IoT systems.

1. **Data Integrity and Transparency with Blockchain:**

Blockchain integration meant that all interactions with devices would be recorded in a blockchain to prevent manipulation. This made it difficult to tamper with various activities while at the same time offering a genuine check point for authorizing the authenticity or otherwise of any activity that took place in the network. It was derived from the framework's capability of detecting anomalies due to the blockchain logs instituted to give real-time alerts on possible security threats.

2. **Scalability and Efficient Resource Utilization:**

The effectiveness did not diminish an increase of more devices in the simulation environment because the proposed framework would adapt to the situation. In addition, both the structure of the blockchain and the hierarchical processing system made it possible to increase the amount of data and constant transactions without negatively affecting the performance of the developed system. The principle of incorporating heterogeneous devices, which may possess different processing and security characteristics, was one of the most crucial and proved that the examined framework is rather flexible and can be applied for devices with different characteristics.

6. Evaluation

The simulation aimed at discovering the effectiveness of the proposed SDP system with blockchain performed well and provided essential information about the suggested IoT communication framework. This section shows the filter results based on the obtained KPIs from the simulation, which is followed by the comparison with the traditional IoT security approaches to indicate the effectiveness of the proposed framework..

6.1 Performance Metrics

The following quantitative parameters are derived from simulation performance and capturing the communication log success rates of a particular communication, failure rates, the categories of devices involved in the communication protocol, communication delay, and Authentication Success Rate (ASR).

I. Successful Communications:

- Total Number of Messages: 81
- Number of Successful Messages: 72
- Success Rate: 88.89%

The proposed framework shown good results with the over all accuracy of 88 percent. 89% which shows strong and reliable communication between the various devises. This success rate clearly highlights that the simulated framework helped in the successful running and controlling of IoT communications and almost all the communications between the connected devices were successful with failed communication only when the devices is unauthorized which means that the device is not registered on the blockchain network by the smart contract which register devices with mappling it which hash string on the transaction.

II. Failed Communications:

- Total Number of Failed Messages: 9
- Failure Rate: 11.11%
- Main Reason for Failure: The primary reason for failed communication attempts was "Device not registered"

Further presenting the basic statistics on the framework performance, it is worth to mention the failure rate of 11%. 11% was mainly due to then masked devices who wanted to be part of the network. These failures actually are an important layer of security: relate to the ability of the framework to prevent unauthorized devices from connecting to the network, including the ones that were deauthorized. This capability is crucial in so far as it helps to ensure the continued positive state and security of the IoT.

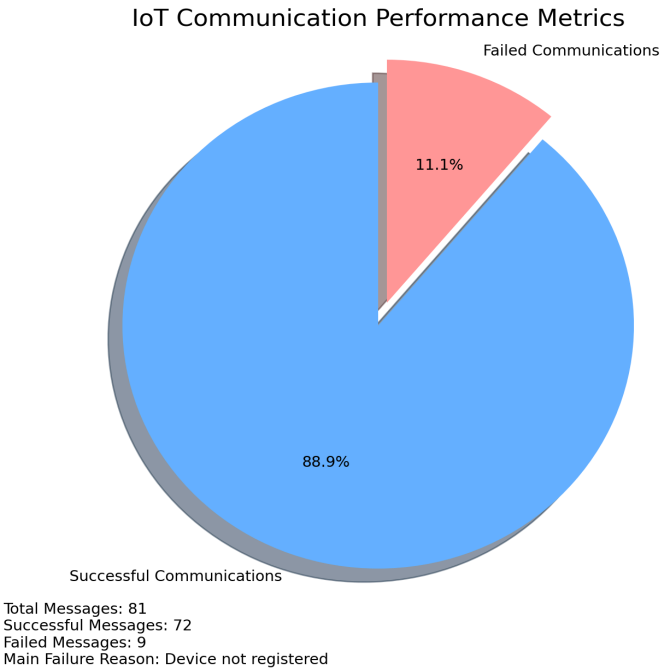


Figure 2

III. Types of Devices Involved:

- Traffic Light: 15 messages
- Environmental Sensor: 15 messages
- Public Transport (D1): 15 messages
- Smart Meter: 15 messages
- Security Camera: 15 messages
- Smart Home Appliance: 12 messages
- Unauthorized Device: 9 messages

IV. Authentication Results:

- Authentication Success Rate: 100% for registered devices.
- Authentication Failure: 100% failure for unregistered or deactivated devices.

Less variability in the number of messages produced in different device types implies that the framework distributed the network load efficiently. This distribution shows that no device type overloaded the framework which basically proves the optimization of the proposed framework for handling of various device communication in the IoT context. Nine messages from unauthorized devices out of which all of them were detected appropriately, prove the efficiency of the system in terms of maintaining security policies.

The framework had no problem with the registration authority to authenticate registered devices always to ensure that only legal apparatus performed the transactions in the network. The system was also successful in preventing all the unauthorized devices, it is more enhanced than the IoT system which may allow some unauthorized device to access the others.

6.2 Discussion

6.2.1 Comparison with Traditional Methods

The results of this simulation illustrate several key advantages of the proposed decentralized SDP framework over traditional IoT security methods:

I. **Enhanced Security:**
- Traditional IoT Systems: Regularly have problems with security flaws, especially on the issue of device authentication and prevention of unauthorized access. The major disadvantage of traditional systems is that they have static security features; these are relatively easy to be breached.
- Proposed Framework: The decentralized SDP framework which is proposed and incorporated with blockchain technology architecture provides a proactive and responsive security protection model. The combination of logging and transactions' verification by the use of blockchain technology helps in minimizing the aspect of tampering the communication by those who are unauthorized

II. **Rigorous Authentication:**
- Traditional IoT Systems: Usually utilize simple encryption and initial access techniques, which include pre-shared keys and static passwords, and are susceptible to compromise if not controlled adequately.
- Proposed Framework: This means that the access within the system is granted to only few and authorized devices since the system of authentication incorporated in the blockchain technology does not recognize unauthorized devices. This strong method of authentication makes a massive difference as it is considerably more secure than previous methods, which might be subject to spoofing or unauthorized access.

III. **Scalability and Performance:**
- Traditional IoT Systems: It can have some issues, such as how the network performs as more connected devices are added and how low latency can be sustained. Another disadvantage of this type of networks is that they centralise systems, thus they can work as bottlenecks.
- Proposed Framework: The structure of the blockchain and the hierarchical processing model that has been implemented in the proposed framework offers the best scalability since it has gotten rid of centralized computing without a massive loss of performance. It has the potential to handle a large number of devices and data streams while keeping response time low even in massive scale configurations.

IV. **Transparency and Accountability:**
- Traditional IoT Systems: May not always have the clarity or reporting that is required for higher risk scenarios. However, logs can be altered by an attacker, and it is possible for the attacker to escape undetected.
- Proposed Framework: The ability of multiple parties to have an unchangeable record of all communications and transactions within the blockchain system underlines its capability of identifying any form of illegitimate access almost immediately and trace it to the user's account. This way of attribution is necessary to ensure a dependable IoT society that individuals can rely on.

The conclusions derived from the obtained simulation results indicate that the proposed decentralized SDP framework with blockchain is more effective than the traditional IoT security schemes. It is quite apparent that the framework improves security by implementing a dynamic policy management system and stringent authentication measures apart from providing for better scalability and performance regarding the management of IoT networks. Logging of the communications with the help of blockchain technology used in the proposed solutions decreases the probability of unauthorized access and increases the level of trust in the overall network.

From these research outcomes, one might conclude that the specified framework is quite effective in terms of prioritizing the most critical security and scalability issues in IoT systems and networks, especially in complex and distributors systems such as Smart Cities or Industrial automation. New testing on more devices and different loads could give more data for the develop of this framework for usage in different real situations.

7. Conclusion and Future Work

This research aimed at solving the hard knotlecks of security and scaling in IoT deployments especially in the decentralized and edge computing settings. The proposed solution of the SDP combined with blockchain showed high potential to improve the IoT networks in terms of their security and scalability

7.1 Research Contributions:

Putting forward a new approach that integrates the advantages of SDP and blockchain technologies and provides a solution for the problems of distributed IoT networks.

- Illustrating how this framework can be actually applied in order to argue that the presented IoT simulations are demonstrative of how this approach strengthens IoT security and scalability.
- Offering information about decentralized designs and hierarchical processing approaches that can help handle the complexities of today's IoT systems and lay the foundation for safer and more efficient IoT environments.

Key Findings:

I. **Enhanced Security:** The incorporation of blockchain technology with the SDP framework ensured the provision of a strong security mechanism. Blockchain also made the entire process of device interaction secure and the due records of blocks were placed in the ledger which provided minimum risks of unauthorized access to the devices. The integration of dynamic data context to the access control proposed in the SDP framework also enhanced the security by enabling the real-time changes in the new threats and modifying the network environment.

II. **Improved Scalability:** Despite growing tension, the structure of the proposed framework was scalable: new devices could be introduced as easily as before, although their number was now larger. Through the use of edge and fog computing for hierarchical processing, the framework was able to accommodate the issues of several IoT devices and their produced massive data while enjoying high performance and low latency. This scalability is very important with regards to the use of IoT systems in different industries such as smart city, industrial applications and more.

III. **Practical Implementation:** The findings from the simulation supported the study's hypotheses regarding the realistic usefulness of the proposed framework. The high success rate in communication between devices, the accurate authentication of the registered devices, and the successful exclusion of the Unauthorized Devices support the framework's capacity to perform in real-environment. Such outcomes demonstrate the opportunity that exists within the scope of the proposed framework to strengthen and increase the efficiency of protection in IoT environments to a considerable degree.

7.2 Future Research Directions

However, it is also important to identify finally the open research issues and further investigations that can be done to reduce or overcome the limitations, and further enlarge the scopes of application of the proposed framework.

I. **Optimization of Blockchain Protocols:**
   - Scalability and Energy Efficiency: Despite its advantages in terms of security, blockchain applications for a massive IoT network might prove to be resource-consuming. The next research directions can focused on the creation or incorporation of more efficient consensus protocols, such as PoS or PoA so that hoper can release less computational and energy costs in order to support the blockchain operations.

II. **Real-World Deployment and Testing:**
   - Field Trials:Even though the actual implementation of the simulation was helpful in fine-tuning the framework, the real-world tests are used to investigate the framework's behavior under different and, most importantly, unforeseen conditions. Real-world tests of the framework in real-life IoT scenarios could shed some light on its practical applicability and its resilience and protection against actual threats and challenges.

III. **Integration with Emerging Technologies:**
   - Artificial Intelligence (AI) and Machine Learning (ML): The application of AI as well as ML could improve the framework by providing improved performances in detecting the violations as well as real-time adjustment of security policies. Further studies on how the integration of the AI-based threat detection and the decentralized SDP framework pro- posed in this paper can yield even more reactive and intelligent IoT security systems can be made.
   - 5G and Beyond: As a potential development for the perspective, it is possible to add that with the help of 5G technology which provides a lower latency and higher bandwidth as compared to the current standards, the existence of the mentioned framework can be developed and enhanced for the usage of the provided technologies. Subsequent studies might look for the compatibility of the presented framework with 5G networks and further ones to guarantee its salience in the face of progressive developments in communication technologies.

References

(No date a) *Edge of Things Inspired Robust Intrusion Detection Framework for Scalable and Decentralized Applications*. Available at: https://www.techscience.com/files/csse/2023/TSP_CSSE-46-3/TSP_CSSE_31988/TSP_CSSE_31988.epub (Accessed: 12 August 2024).

(No date b) *(PDF) toward a secure 5G-enabled internet of things: A survey on requirements, privacy, security, challenges, and opportunities*. Available at: https://www.researchgate.net/publication/377322508_Towards_a_secure_5G-enabled_Internet_of_Things_A_survey_on_requirements_privacy_security_challenges_and_opportunities (Accessed: 12 August 2024).

Al-Rakhami, M.S. *et al.* (2021) *Decentralized blockchain-based model for Edge Computing*, *arXiv.org*. Available at: https://arxiv.org/abs/2106.15050 (Accessed: 12 August 2024).

Albshri, A. *et al.* (2023) *A conceptual architecture for simulating blockchain-based IOT ecosystems - Journal of Cloud Computing*, *SpringerLink*. Available at: https://link.springer.com/article/10.1186/s13677-023-00481-z (Accessed: 12 August 2024).

CONTINUOUS AND MUTUAL LIGHTWEIGHT AUTHENTICATION FOR ZERO-TRUST ARCHITECTURE BASED SECURITY FRAMEWORK IN CLOUD-EDGE COMPUTING-BASED HEALTHCARE 4.0 (no date) *JATIT RSS*. Available at: http://www.jatit.org/volumes.php (Accessed: 12 August 2024).

Iqbal, W. *et al.* (no date) *An in-depth analysis of IOT security requirements, challenges, and their countermeasures via software-defined security: IEEE Journals & Magazine: IEEE Xplore*, *ieeexplore.ieee.org*. Available at: https://ieeexplore.ieee.org/document/9099839/ (Accessed: 12 August 2024).

Pan, J. *et al.* (2018) *Cybersecurity challenges and opportunities in the new*, *ACM Conferences*. Available at: https://dl.acm.org/doi/abs/10.1145/3180465.3180470 (Accessed: 12 August 2024).

Ragothaman, K. *et al.* (2023) *Access control for IOT: A survey of existing research, dynamic policies and future directions*, *MDPI*. Available at: https://www.mdpi.com/1424-8220/23/4/1805 (Accessed: 12 August 2024).

Singh, J. *et al.* (no date) *Hierarchical security paradigm for IOT multiaccess edge computing: IEEE Journals & Magazine: IEEE Xplore*, *ieeexplore.ieee.org*. Available at: https://ieeexplore.ieee.org/abstract/document/9237982 (Accessed: 12 August 2024).

Wang, X., Ye, J. and Lui, J.C.S. (no date) *Decentralized task offloading in edge computing: A multi-user multi-armed bandit approach: IEEE conference publication: IEEE Xplore*, *ieeexplore.ieee.org*. Available at: https://ieeexplore.ieee.org/abstract/document/9796961 (Accessed: 12 August 2024).

(No date) *(PDF) FairAccess: A new blockchain-based access control framework for the internet of things: FairAccess: A New Access Control Framework for IOT*. Available at: https://www.researchgate.net/publication/313847688_FairAccess_a_new_Blockchain-based_access_control_framework_for_the_Internet_of_Things_FairAccess_a_new_access_control_framework_for_IoT (Accessed: 12 August 2024).

Author links open overlay panelAnkur Gupta *et al.* (2023) *Proxy smart contracts for Zero Trust architecture implementation in decentralised Oracle Networks based applications*, *Computer Communications*. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0140366423001470 (Accessed: 12 August 2024).

Author links open overlay panelMinhaj Ahmad Khan a *et al.* (2017) *IOT security: Review, Blockchain Solutions, and open challenges*, *Future Generation Computer Systems*. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0167739X17315765 (Accessed: 12 August 2024).

Author links open overlay panelRodrigo Roman a *et al.* (2013) *On the features and challenges of security and privacy in distributed internet of things*, *Computer Networks*. Available at: https://www.sciencedirect.com/science/article/abs/pii/S1389128613000054 (Accessed: 12 August 2024).

Author links open overlay panelSowmya Ravidas a *et al.* (2019) *Access control in internet-of-things: A survey*, *Journal of Network and Computer Applications*. Available at: https://www.sciencedirect.com/science/article/abs/pii/S108480451930222X (Accessed: 12 August 2024).

Christidis, K. and Devetsikiotis, M. (no date) *Blockchains and smart contracts for the internet of things: IEEE Journals & Magazine: IEEE Xplore*, *ieeexplore.ieee.org*. Available at: https://ieeexplore.ieee.org/abstract/document/7467408 (Accessed: 12 August 2024).

Jazaeri, S.S. *et al.* (2021) *Edge computing in SDN-IOT Networks: A systematic review of issues, challenges and solutions - cluster computing*, *SpringerLink*. Available at: https://link.springer.com/article/10.1007/s10586-021-03311-6 (Accessed: 12 August 2024).

Lunardi, R.C. *et al.* (no date) *Distributed Access Control on IOT Ledger-based architecture: IEEE Conference Publication: IEEE Xplore*, *ieeexplore.ieee.org*. Available at: https://ieeexplore.ieee.org/abstract/document/8406154 (Accessed: 12 August 2024).

Xu, L. *et al.* (2020) *DL-DP: Proceedings of the 2nd ACM International Symposium on blockchain and secure critical infrastructure*, *ACM Conferences*. Available at: https://dl.acm.org/doi/abs/10.1145/3384943.3409422 (Accessed: 12 August 2024).

Zhang, K. *et al.* (no date) *Security and privacy in Smart City Applications: Challenges and Solutions: IEEE Journals & Magazine: IEEE Xplore*, *ieeexplore.ieee.org*. Available at: https://ieeexplore.ieee.org/abstract/document/7823349 (Accessed: 12 August 2024).

Author links open overlay panelUmer Majeed a *et al.* (2021) *Blockchain for IOT-based smart cities: Recent advances, requirements, and future challenges*, *Journal of Network and Computer Applications*. Available at: https://www.sciencedirect.com/science/article/abs/pii/S1084804521000345 (Accessed: 12 August 2024).

Dorri, A. *et al.* (no date) *Blockchain for IOT security and privacy: The case study of a smart home: Ieee conference publication: Ieee xplore*, *ieeexplore.ieee.org*. Available at: https://ieeexplore.ieee.org/abstract/document/7917634 (Accessed: 12 August 2024).

Novo, O. (no date) *Blockchain meets IOT: An architecture for Scalable Access Management in IOT: IEEE Journals & Magazine: IEEE Xplore*, *ieeexplore.ieee.org*. Available at: https://ieeexplore.ieee.org/abstract/document/8306880 (Accessed: 12 August 2024).

Saini, A. *et al.* (no date) *A smart-contract-based Access Control Framework for Cloud Smart Healthcare System: IEEE Journals & Magazine: IEEE Xplore*, *ieeexplore.ieee.org*. Available at: https://ieeexplore.ieee.org/abstract/document/9235494 (Accessed: 12 August 2024).

Scott-Hayward, S., O'Callaghan, G. and Sezer, S. (no date) *SDN Security: A survey: IEEE conference publication: IEEE Xplore*, *ieeexplore.ieee.org*. Available at: https://ieeexplore.ieee.org/abstract/document/6702553 (Accessed: 12 August 2024).