OULU 2023
C 914

ACTA UNIVERSITATIS OULUENSIS

Tharaka Hewa

EFFICIENT DECENTRALIZED SECURITY SERVICE ARCHITECTURE FOR INDUSTRIAL IOT

UNIVERSITY OF OULU GRADUATE SCHOOL;
UNIVERSITY OF OULU,
FACULTY OF INFORMATION TECHNOLOGY AND ELECTRICAL ENGINEERING

ACTA UNIVERSITATIS OULUENSIS
C Technica 914

THARAKA HEWA

EFFICIENT DECENTRALIZED SECURITY SERVICE ARCHITECTURE FOR INDUSTRIAL IOT

Academic dissertation to be presented with the assent of the Doctoral Programme Committee of Information Technology and Electrical Engineering of the University of Oulu for public defence in the OP auditorium (L10), Linnanmaa, on 4 December 2023, at 12 noon

UNIVERSITY OF OULU, OULU 2023

Acta Univ. Oul. C 914, 2023

Supervised by
Professor Mika Ylianttila
Docent Madhusanka Liyanage
Docent Pawani Porambage

Reviewed by
Professor Raja Jurdak
Professor Nirupama Bulusu

Opponent
Professor Karl Andersson

ISBN 978-952-62-3913-2 (Paperback)
ISBN 978-952-62-3914-9 (PDF)

ISSN 0355-3213 (Printed)
ISSN 1796-2226 (Online)

Cover Design
Raimo Ahonen

PUNAMUSTA
TAMPERE 2023

Hewa, Tharaka, Efficient decentralized security service architecture for Industrial IoT
University of Oulu Graduate School; University of Oulu, Faculty of Information Technology and Electrical Engineering
Acta Univ. Oul. C 914, 2023
University of Oulu, P.O. Box 8000, FI-90014 University of Oulu, Finland

Abstract

The current evolution of industrial systems is characterized by expectations of increased production efficiency, data security, regulatory compliance, scalability, and environmental sustainability. One of the key technologies driving these advancements is the Industrial Internet of Things (IIoT), together with 5th Generation(5G) and beyond networks. These enable seamless connectivity between infrastructure, machines, and people, facilitating rapid data exchange, automation, monitoring, and control of industrial systems.

In this thesis, the main contributions are threefold. First, the thesis proposes a novel decentralized service architecture to establish confidentiality, integrity, and authentication of cloud-integrated IIoT. Secondly, the research proposed a decentralized architecture incorporating Game Theory for efficient and secured network slice brokering and service-level agreement establishment. Finally, the thesis proposed a novel consensus mechanism for reliable IIoT data formulation. This thesis proposes to utilise reputation score as a numerical indicator for the IIoT data reliability in combination with BulletProof zero-knowledge proof to defend the data formulation IIoT from slowly adaptive adversaries to yield energy efficiency. Identifying the scalability limitations in the centralized security services, the thesis incorporated blockchain-based smart contracts as a decentralized service enabler that provides decentralization, lower latency, and transparency with cryptographically integrity-preserved ledger.

The proposed service architecture was implemented and evaluated with numerical and programmatic simulations. The thesis results were derived from the comparisons of partial implementations from state-of-art to distinguish the numerical advantages of the proposal. The proposed architecture has yielded significant efficiency improvements, including storage utilization (to 20% in IIoT authentication), latency (Up to 55% in IIoT authentication), resource offer pricing (Up to 21% in slice requests), and energy consumption (Up to 53% in reputation score verification) beyond key state-of-art. In addition, the proposed consensus protocol in the thesis was verified for robustness of chain growth in attack scenarios.

Keywords: 5G, blockchain, consensus, efficiency, IIoT

Hewa, Tharaka, Tehokas hajautettu tietoturvapalveluarkkitehtuuri teolliselle esineiden Internetille
Oulun yliopiston tutkijakoulu; Oulun yliopisto, Tieto- ja sähkötekniikan tiedekunta
Acta Univ. Oul. C 914, 2023
Oulun yliopisto, PL 8000, 90014 Oulun yliopisto

Tiivistelmä

Teollisten järjestelmien nykykehitykselle on ominaista odotukset tuotannon tehostamisesta, tietoturvasta, säännösten noudattamisesta, skaalautuvuudesta ja ympäristön kestävyydestä. Yksi tähän kehitykseen johtavista keskeisistä teknologioista on teollinen esineiden internet (IIoT) yhdessä viidennen sukupolven (5G) ja muiden verkkojen kanssa. Ne mahdollistavat saumattoman yhteyden infrastruktuurin, koneiden ja ihmisten välillä, mikä helpottaa nopeaa tiedonvaihtoa, automaatiota, valvontaa ja teollisten järjestelmien hallintaa.

Tämän väitöstutkimuksen tärkeimmät tulokset ovat kolmella alueella. Ensinnäkin työssä ehdotetaan uutta hajautettua palveluarkkitehtuuria pilvilaskentaan integroidun IIoT:n luottamuksellisuuden, eheyden ja todentamisen varmistamiseksi. Toiseksi tutkimuksessa ehdotetaan hajautettua arkkitehtuuria, joka hyödyntää peliteoriaa tehokkaan ja suojatun verkon viipaloinnin välitys- ja palvelutasosopimuksen toteuttamiseksi. Lopuksi työssä ehdotetaan uutta konsensusmekanismia luotettavaa IIoT-tietojen laatimista varten. Tässä tutkimuksessa ehdotetaan mainepisteiden hyödyntämistä numeerisena indikaattorina IIoT-tietojen luotettavuudelle yhdessä BulletProof-tietokannan kanssa, joka puolustaa datan luomista IIoT järjestelmissä hitaasti mukautuvilta hyökkäyksiltä, energiatehokkuuden huomioiden. Keskitettyjen turvallisuuspalvelujen skaalautuvuusrajoitukset huomioiden, lohkoketjupohjaiset älykkäät sopimukset sopivat hajautetuksi palvelun mahdollistajaksi, joka tarjoaa hajauttamisen, pienemmän viiveen ja läpinäkyvyyden kryptografisesti eheyden säilyttävällä tilikirjalla.

Ehdotettu palveluarkkitehtuuri toteutettiin ja arvioitiin numeerisilla ja ohjelmallisilla simulaatioilla. Väitöstutkimuksen tulokset on johdettu vertaamalla osatoteutusta uusinta tekniikkaa erottamaan ehdotuksen numeeriset edut. Ehdotettu arkkitehtuuri on tuottanut merkittäviä tehokkuusparannuksia, joita ovat muun muassa tallennuksen käyttö (20 prosenttiin IIoT-todennuksessa), viive (55 prosenttiin IIoT-todennuksessa), resurssitarjonnan hinnoittelu (21 prosenttiin viipalointipyynnöissä) ja energiankulutus (53 prosenttiin mainepisteiden verifioinnissa) nykytoteutuksiin verrattuna. Lisäksi opinnäytetyössä ehdotettu konsensusprotokolla todennettiin, siten että ketjun kasvu on vakaata hyökkäysskenaarioissa.

Asiasanat: 5G, esineiden internet, konsensusalgoritmit, lohkoketjutekniikat, tehokkuus, turvallisuus

To my family.

Acknowledgements

This research has been carried out in Network Security, Trust, and Privacy(NetSEC) research group of the Networks and Systems research unit at the Centre for Wireless Communication (CWC), at the University of Oulu, in Finland. The thesis has been financially supported by the Academy of Finland 6Genesis Flagship (grant 346208), EU INSPIRE-5Gplus Project (grant no. 871808), SecureConnect, and 6GCURE projects.

The thesis is also financially supported by the Foundations of Nokia, TES,Tauno Tonning, Riitta and Jorma J. Takanen. I would like to thank my supervisor Prof. Mika Ylianttila for his tremendous guidance and support throughout my studies. I would also like to extend my sincere gratitude to the co-supervisor Dr. Madhusanka for the active contribution and valuable technical feedback on the research publications. I want to thank Dr. Pawani Porambage for the support and her active role as the project manager and a co-supervisor. I convey my special thanks to Prof. An Braken on sharing her expertise in cryptography to improve the research. My special thanks go to the follow-up group committee consisting of Associate Prof. Hirley Alves and Assistant Prof. Sumudu Samarakoon for providing their valuable comments on this thesis. I owe my thanks to Prof. Nandana Rajatheva for sharing his valuable thoughts with me to carry out my doctoral studies.

The work in this thesis was partly conducted during the research visits I made to the Vrije Universiteit Brussel in Brussels, Belgium and University College Dublin, Ireland. I want to thank Prof. An Breaken and Dr. Madhusanka Liyanage for hosting my short research visits and for providing valuable comments on the work during the stays. Moreover, I would like to thank all the co-authors of my publications for their noteworthy contributions and cooperation. I convey my gratitude to my official reviewers, Prof. Raja Jurdak and Prof. Nirupama Bulusu for providing valuable and constructive comments. I would also like to thank Prof. Karl Andersson for serving as the opponent in the doctoral defense. I received great deal of support from all my colleagues, including Yushan, Nisita, and Janani.

I want to express my heartiest gratitude to my friends, Nuwan and Chanaka from Oulu. I also thank Dr. Chathuranga and Dr. Jayampathi from CWC staff for sharing their experiences in research career. I want to extend my gratitude towards the close faculty members of University of Colombo School of Computing Sri Lanka, including

Mr. Gihan Seneviratne, and Prof. Kasun de Zoysa for their immense motivation to switch for higher studies and eventually follow PhD. I sincerely thank Prof. Wee Keong Ng from Nanyang Technological University, Singapore, for opening up my research career while working as a senior software engineer in Sri Lanka. I am much thankful to Dr. Newton Fernando from Nanyang Technological University, Singapore, for providing tremendous motivation by sharing his experiences in his research career.

My special thanks go also to my friends, relatives, and parents-in-law for supporting me throughout this journey. I would deeply like to thank my ever-loving parents for giving me so much the courage and making me whom I am today. Finally, I convey my heartiest gratitude to my wife, Nilushika for her support in the past four years.

Tharaka Hewa
02.11.2023

List of abbreviations

5G	*5th Generation*
6G	*6th Generation*
AR	*Augmented Reality*
CA	*Certification Authority*
CRL	*Certification Revocation List*
CM	*Cloud Manufacturing*
CoAP	*Constrained Application Protocol*
CSP	*Cloud Service Provider*
DH	*Diffie-Hellman*
DoS	*Denial of Service*
DDoS	*Distributed Denial of Service*
ECC	*Elliptic Curve Cryptography*
ECDHP	*Elliptic Curve Diffie Hellman Problem*
ECDLP	*Elliptic Curve Discrete Logarithm*
ECQV	*Elliptic Curve Qu Vanstone*
ECIES	*Elliptic Curve Integrated Encryption Scheme*
eMBB	*Enhanced Mobile Broadband*
GDPR	*General Data Protection Regulation*
HIPAA	*Health Insurance Portability and Accountability Act*
IDS	*Intrusion Detection System*
IES	*International Electrotechnical Commission*
IETF	*Internet Engineering Task Force*
IoT	*Internet of Things*
IIoT	*Industrial Internet of Things*
IIRA	*Industrial Internet Reference Architecture*
LoRa	*Long Range*
M2M	*Machine to Machine*
MiTM	*Man in The Middle*
mMTC	*Massive Machine Type Communications*
MNO	*Mobile Network Operator*
MQTT	*Message Queuing Telemetry Transport*
MVNO	*Mobile Virtual Network Operator*
NIZKP	*Non-Interactive Zero Knowledge Proof*
NIST	*National Institute of Standards and Technology*

NSB	*Network Slice Broker*
OTT	*Over the Top*
PKI	*Public Key Infrastructure*
RAN	*Radio Access Network*
RP	*Resource Provider*
RSU	*Road Side Units*
SDG	*Sustainable Development Goals*
SFSBroker	*Secured and Federated Slice Broker*
SSB	*Security Service Blockchain*
SSLA	*Secured Service Level Agreement*
TCP	*Transmission Control Protocol*
TTP	*Trusted Third Party*
UDP	*User Datagram Protocol*
UN	*United Nations*
URLLC	*Ultra-Reliable Low Latency Communications*
VR	*Virtual Reality*
WAN	*Wide Area Network*
WLAN	*Wireless Local Area Network*
ZKP	*Zero Knowledge Proof*
zkSNARK	*Zero-Knowledge Succinct Non-Interactive Argument of Knowledge*

List of original publications

This thesis is based on the following publications, which are referred throughout the text by their Roman numerals:

I Hewa T, Braeken A, Ylianttila M & Liyanage M “Blockchain-Based Automated Certificate Revocation for 5G IoT.” ICC 2020 - 2020 IEEE International Conference on Communications (ICC), IEEE, 2020, pp. 1–7. DOI.org (Crossref), https://doi.org/10.1109/ICC40277.2020.9148820.

II Hewa T, Braeken A, Liyanage M & Ylianttila M. “Fog Computing and Blockchain-Based Security Service Architecture for 5G Industrial IoT-Enabled Cloud Manufacturing.” IEEE Transactions on Industrial Informatics, vol. 18, no. 10, Oct. 2022, pp. 7174–85. DOI.org (Crossref), https://doi.org/10.1109/TII.2022.3140792.

III Hewa T, Kalla A, Porambage P, Liyanage M & Ylianttila M “How DoS Attacks Can Be Mounted on Network Slice Broker and Can They Be Mitigated Using Blockchain?” 2021 IEEE 32nd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), IEEE, 2021, pp. 1525–31. DOI.org (Crossref), https://doi.org/10.1109/PIMRC50174.2021.9569375.

IV Hewa T, Porambage P, Kovacevic I, Weerasinghe N, Harjula E,Liyanage M & Ylianttila M. “Blockchain-Based Network Slice Broker to Facilitate Factory-As-a-Service.” IEEE Transactions on Industrial Informatics, vol. 19, no. 1, Jan. 2023, pp. 519–30. DOI.org (Crossref), https://doi.org/10.1109/TII.2022.3173928.

V Hewa T, Porambage P, Kalla A, Pamela D, Liyanage M & Ylianttila M. “Blockchain and Game Theory Convergence for Network Slice Brokering.” Computer, vol. 56, no. 3, Mar. 2023, pp. 80–91. DOI.org (Crossref), https://doi.org/10.1109/MC.2022.3165533.

VI Hewa T, Braeken A, Porambage P, Liyanage M & Ylianttila M. “ Bulletproofs based Novel Privacy-preserved Consensus Protocol for 5G connected IoT Data ” Journal article manuscript submitted to IEEE Transactions on Network and Service Management

Contents

1 Introduction

1.1 Rationale of the research

Industry 4.0 integrates digital technologies to advance the quality of living, enhance economic growth, and drive industries towards global sustainability [1] with automated manufacturing and industrial processes. Enterprises gain increased manufacturing efficiency, data-driven decision-making, data-driven analysis, and improved resource utilization, leading to maximizing business value and productivity through the recent evolution of industrial systems. The Internet of Things (IoT), a game changer in automation in recent years, interconnects various infrastructures, including home appliances, manufacturing equipment, medical actuators, and monitoring equipment, with provisions for seamless and real-time information exchange. The emergence of computing power decentralization through the evolution of edge and fog computing promises significant advancements with enhanced data privacy, reduced latency, and increased bandwidth efficiency.

The evolution of 5th Generation(5G) and beyond telecommunication extends the capabilities of IoT with higher network capacity to connect a massive number of nodes simultaneously for data exchange. 5G networks cater to connectivity in three distinguishing service categories as Enhanced Mobile Broadband(eMBB), Ultra-Reliable Low Latency Communications (URLLC), and Massive Machine Type Communications (mMTC). eMBB enhances mobile broadband with high data rates to connect bandwidth-intensive applications such as Virtual Reality (VR), Augmented Reality (AR), and Ultra-High-Definition (UHD) video streaming in industrial applications such as the real-time visualization of analytics using VR, remote maintenance, and telemedicine. URLLC provide reliable and real-time communication for critical safety applications such as vehicular networks that utilize automated collision avoidance functions, smart grids that communicate in real-time with power distribution points, and industrial control systems that require high-speed connectivity. mMTC facilitates connectivity in massive-scale machine-to-machine communication with compatibility with many IoT devices in a single network to exchange data in real time. mMTC facilitates various industry verticals, including smart manufacturing, healthcare, agriculture, and supply chain management.

The Industrial Internet of Things(IIoT) has emerged as an industry-specific specialized variant of IoT. IIoT addresses the unique requirements of industrial settings, including manufacturing, transportation, energy, and agriculture. IIoT caters to enterprises with industry-grade robust, efficient, and reliable connectivity for real-time monitoring and automation of industrial processes. Implementing security in communications in IIoT, including security, trust, and privacy [2] are core requirements [3], as the IIoT systems include data processing in the edge[4] and cloud servers [5] with transfers over untrusted networks. The data exchanged between the IIoT sensors, actuators, and associated services must preserve fundamental security requirements, including privacy, integrity, authentication, access control, and non-repudiation. Furthermore, the IIoT systems must comply with industry-specific data protection standards such as the Health Insurance Portability and Accountability Act [6] (HIPAA) and the General Data Protection Regulation [7] (GDPR) to defend the sensitive information against malicious and curious parties with ensured confidentiality, integrity, and availability. IIoT data privacy ensures that the exchanged messages do not reveal significant insights to malicious parties over the network. Data integrity ensures the exchanged data is not manipulated by adversaries in the network. Access control defines the authorized personnel and the services to access the IoT services and data. Security is considered a design goal and core requirement in IoT system design.

Implementing IIoT security is a significant challenge as the deployment models, communication protocols, computational capabilities, different vendor architectures [8, 9], and functional requirements are heterogeneous in IIoT networks. Furthermore, IIoT systems require scalability, reliability, and performance features such as real-time data transfers and low-latency communication. For example, end-to-end encryption must not incur significant latency for the real-time video streaming of telehealth service via healthcare IIoT systems. The IIoT nodes are heterogeneous, lacking computational power to process expensive cryptographic operations. For example, 2048-bit Rivest–Shamir–Adleman(RSA) encryption is a computationally expensive operation for some hardware in IIoT [10]. In addition, the communication overhead increases when the IIoT systems elevate the security standards. For example, frequent key exchange is a potential solution to reduce the impact of key compromise. However, the increased key exchange frequency incurs additional communication overhead on the network, proportional to the number of IIoT tenants. Enabling interoperability[11] is another requirement so that IIoT can function collaboratively with existing services such as cloud and edge. Implementing security standards, compliance, and regulations on a heterogenous infrastructure like IIoT is significantly challenging [12] as the networks are larger in scale than consumer IoT networks.

The state-of-the-art IoT security service architectures, including Public Key Infrastructure(PKI), follow centralized service models[13] to align with the centralized architecture with cloud-based processing power and storage. However, the future evolutionary directions of computing decentralize the computational power to the intermediary layers from the end users and cloud servers [14] expecting intermediary data processing and storage closer to the IIoT devices. Machine-to-machine (M2M) communication and distributed machine learning services like federated learning are potential prominent technologies to leverage the higher transaction volume processing of the future IIoT systems. From a security perspective, decentralized service models ensure availability and resistance to Denial of Service Attacks/Distributed Denial of Service(DoS/DDoS) attacks for centralized systems[15].

Blockchain and smart contacts are renowned as the game changers of the decade, with the establishment of a collaborative digital platform that securely records and verifies transactions between multiple participants. Initially, the blockchain concept was introduced for the financial transactions of the Bitcoin network by Satoshi Nakamoto in 2008[16]. The concept of the smart contract is an extension of the principles of blockchain with an immutable program execution capability within the member network. However, blockchain and smart contracts provide a strong potential to adapt to the industrial applications than financial ones. The unique capabilities of blockchain and smart contracts leverage the multiple IoT security services with decentralization capabilities with the extended capability to handle a massive transaction volume.

The blockchain forms a decentralized, immutable ledger comprising a cryptographically linked chain of blocked records. The record collections are approved using a consensus mechanism. The distributed consensus mechanism and the cryptographically integrity preserved ledger make the blockchain more robust to the adversaries[17] when compared with the centralized service architectures. The fundamental component of a block is a transaction. Each block consists of primary information fields, including the block sequence number, block header, Merkle root hash, and the block signature. The array of blocks formulates cryptographic links between each block and ensures the integrity of blocks and transactions are preserved based on the principles of cryptography. Smart contracts enable the consistent deployment of services to operate on a decentralized infrastructure layer. In general, the blockchain and smart contracts provide a platform for the decentralized deployment of security service functions encoded as smart contracts. The decentralized deployment of security services as smart contract deployment provides reduced latency and improved scalability for future IIoT networks. Blockchain facilitates the industry verticals such as IoT trust establishment and the supply chain [18, 19] with its own unique capabilities.

The operating modes of the blockchain are primary considerations in establishing and integrating the blockchain for enterprise applications. There are two operating modes of blockchain, which are public and consortium type. These define the member onboarding procedure of the network. In a public blockchain, anyone who fulfils the conditions of blockchain network onboarding can connect and contribute to the network. Bitcoin and Ethereum are well-known public blockchain networks. In contrast, the consortium blockchain networks define conditions for connectivity to the blockchain network. For example, for a healthcare data management consortium blockchain, the network members must be domain stakeholders such as medical institutions. The consortium blockchain has more regulation and authority concerning the operating members rather than public blockchain platforms.

Consensus is one of the core principles of the context of blockchain. The consensus mechanism defines the conditions of the members' agreement in approving the blocks of transactions in the ledger. More specifically, the consensus mechanism defines the strategy to select the member and append the block to the ledger. In the consensus process, the electing member of a round must fulfil a publicly provable condition to get the block accepted by the network members.

A significant amount of research from the industry and academia has been conducted in the past decade to investigate the potential applications of blockchain and smart contracts for IIoT security. Blockchain has a significant potential to advance IIoT security due to its decentralized nature, which eliminates the need for a central authority and fosters trust between participants through consensus. It ensures data integrity and authenticity through cryptographic algorithms and immutable records, ensuring integrity, authentication, and non-repudiation by default. The transparent and traceable audit trail created by blockchain enhances monitoring, auditing, and forensic analysis, bolstering IIoT security. Additionally, the decentralized operational capability of smart contracts ideally accommodates potential security services into the edge infrastructure[20]. Overall, blockchain has a significant potential to incorporate security services into decentralized infrastructure while achieving efficiency and scalability, which is required in IIoT. Ultimately, the inherent robustness[21] from the consensus and cryptographically linked ledger motivated this research to utilize the blockchain as the foundation for the service architecture.

However, the state of art blockchain architectures suffer from significant limitations that disrupt the utilization of the distinguishing potential of the blockchain. Imposing privacy over the transaction ledger is a significant challenge as individual IoT security service transaction data is replicated consistently over the members' blockchain instances An adversary can derive important insights when the public ledger data reflects identity information and could link the transaction data to an individual IoT node's security service functions. Furthermore, storage scalability is one of the most important design considerations in blockchain for IoT security, as, in principle, the ledger grows exponentially as the blockchain system evolves. The growing ledger incurs a significant overhead on the blockchain nodes. In addition, 5G and beyond networks rely on the softwarized functions. The blockchain service layer is a versatile platform to secure the softwarized network service functions with lower latency and distributed service capability.

The study examines the obstacles associated with ensuring the security of IIoT networks and the potential of blockchain to alleviate identified challenges from three distinct viewpoints. First, the research identifies the challenges on efficiently authenticating IIoT and IoT-Fog-Cloud key establishment. It proposes a smart contract-based service architecture to authenticate IoT nodes with improved storage efficiency and lower latency. Secondly, the research identifies the potential of network slice brokering. It proposes a DoS/DDoS attack-resistant federated slice brokering framework using smart contracts with improved resource provider utilization and lower consumer pricing. Finally, the research proposes a novel reputation score-based consensus mechanism that utilizes the BulletProof Zero Knowledge Proof(ZKP) for energy-efficient and network resource-efficient verification of the reputation score. A detailed decomposition of the threats and limitations of the state of the art that motivated this research has been presented in Section 4.3.

This research uses IoT and IIoT terms interchangeably as the research proposes potential IoT security services with the implementation and validation on industrial application scenarios.

1.2 Organization of the thesis

This thesis is organized as follows: Chapter 2 presents a background review, including the IoT to IIoT transformation, technical concepts, and cryptographic principles utilized in the research. Chapter 3 reviews the literature, including related works and similar approaches. Chapter 4 discusses a summary of contributions made by this study. Chapter 5 includes a discussion of the research. Chapter 6 concludes the thesis.

2 Background

This chapter presents an overview of the technical background that motivated the research and several cryptographic principles utilized in the study. Section 2.1 provides an introduction to the IoT with the reference architectures. Section 2.2 briefly describes the evolution of IIoT as a specialized version of IoT. Section 2.3 emphasizes the definitions of widely used terms to distinguish the advancement of the proposed work beyond state of the art. Section 2.4 explains the network slicing and slice brokering and the potential applicability in IIoT. Section 3.3 describes the requirement of reliable data formulation in IIoT. Section 2.6 includes descriptions of the widely used authentication and encryption techniques to secure IIoT. Section 2.7 explains the BulletProof mechanism, which is used in privacy-preserved reputation score verification. Section 2.8 explains the preliminary concepts of blockchain and smart contracts. Finally, Section 2.9 explains the applicability of the background concepts to the thesis.

2.1 Introduction to the internet of things

2.1.1 The internet of things

The Internet of Things (IoT) extends the capabilities of physical devices with the integration of embedded electronics to enable program execution. IoT establishes connectivity between devices and cloud services for data collection, processing, storage, and physical device control. The evolution of miniature computational infrastructure, such as low-power microcontrollers and sensors, augmented physical device capabilities, including real-time data acquisition, processing, and transmission. The communication protocols such as Wi-Fi, Bluetooth, and beyond 5G networks promise seamless connectivity between the IoT and associated services such as the cloud with ensured

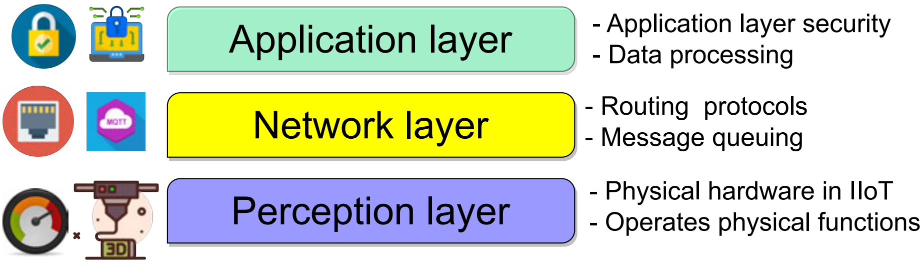

Fig. 1. The three layers of IoT based on (Redrawn based on [22]).

performance requirements. The Internet Engineering Task Force (IETF) proposes a three-layered architecture in [22]. Figure 1 illustrates the three layers of IoT.

- Perception layer: The physical devices such as sensors and actuators correspond to the perception layer. The categories of sensors include temperature sensors, humidity sensors that directly link with a physical function such as production line monitoring in manufacturing and cold chain condition monitoring in the supply chain. The actuators are heterogeneous with different capabilities according to the application. Actuator-type IoT devices include 3D printers and smart home controllers.
- Network layer: The network layer establishes the communication between the perception and application layers. Routing protocols such as TCP UDP and MQTT CoAP operate in the network layer. The implementation of research were conducted on MQTT and TCP-based implementation environments.
- Application layer: The application layer includes the applications and processing of data captured by the perception layer

The application-level security functions developed in this research operate on the application layer.

2.1.2 Designing and securing IoT systems for industry

The high-level architecture of IoT solutions is an important consideration in designing and implementing IoT applications targeted for the industry. Interoperability between the associated services, such as real-time data processing, storage, and transmission, an important consideration in IoT system design.

The IoT reference architecture provides insights into the development of IoT systems. The reference architecture defines the guidelines for IoT deployment, including security specifications and communication protocols. Different vendors propose different IoT security architectures according to their own business specialization. Regardless of the vendor-specific applications, the reference architecture provides important insights into designing the IIoT systems with ensured security.

The IBM-IoT reference architecture [9] defines IBM's approach to IoT solutions. IBM reference architecture emphasizes the requirement of transmission, storage, and analyzing data from sensors using an IIoT platform.The Microsoft Azure IoT reference architecture[8] describes the Azure components and services commonly used. Furthermore, the significance of trustworthy and secure communication with data encryption and digital signatures is also emphasized in these two reference architectures. Microsoft Azure IoT reference architecture also emphasized the potential application of a field gateway that acts as an intermediary to connect constrained IoT devices to the cloud. The WSO2 reference architecture [23] proposes an open-source and project-based vendor-neutral architecture. The reference architecture elaborates on the risks of attacks to IoT systems and the potential of encryption and identity management techniques. In general, scalability is one of the most prominent design considerations in the industrial use cases of IoT, such as large-scale IoT node deployment scenarios. The IoT reference architectures provide important insights to ensure robustness, scalability, security, and interoperability. The perception illustrated in the reference architecture inspired the research to investigate efficient security services for IIoT. The Industrial Internet Consortium proposes the Industrial Internet Reference Architecture (IIRA)[24] that provides blueprints for designing and deploying Industrial IoT solutions. IIRA emphasizes that security, privacy, and reliability are common technical challenges in IIoT. The Open Group proposes the Open Platform 3.0 Architecture [25], which includes basic design models for emerging technologies, including IoT and cloud computing These reference architectures provide a similar framework for designing and implementing IIoT solutions but may differ in their specific layering and components based on the focus and goals of the organization that developed them. Open Platform 3.0 architecture notes that security, scalability, and reliability are foundational capabilities for effective communication. Overall, the IoT security was highlighted as a vital requirement in IoT applications. Figure 2 reflects the IIoT system model in 5G and beyond networks.

IoT connectivity is crucial for the successful function of IoT-integrated services. Reliable and secure communication between the devices and the services deployed in the cloud is essential for collecting, processing, analyzing, and storing data. Interruptions in connectivity will result in transmission delays and catastrophic consequences in critical IoT applications such as healthcare and industrial control systems. The connectivity technologies in IoT are various. Each technology has its capabilities and weaknesses according to different application perspectives. For example, LoRA-WAN and ZigBee are ideal for connecting low-power environmental monitoring systems. The payload size per packet of LoRA WAN is 242 bytes[26], and the packet size of Zig-Bee is 127 bytes[27]. In contrast, WiFi and cellular networks deliver high bandwidth and high data rate connectivity. IoT-connected vehicles for real-time operations require highly reliable and low-latency connectivity. The evolution of 5G and beyond networks promises higher data rates ranging up to Gbps by enabling more sophisticated industrial applications.

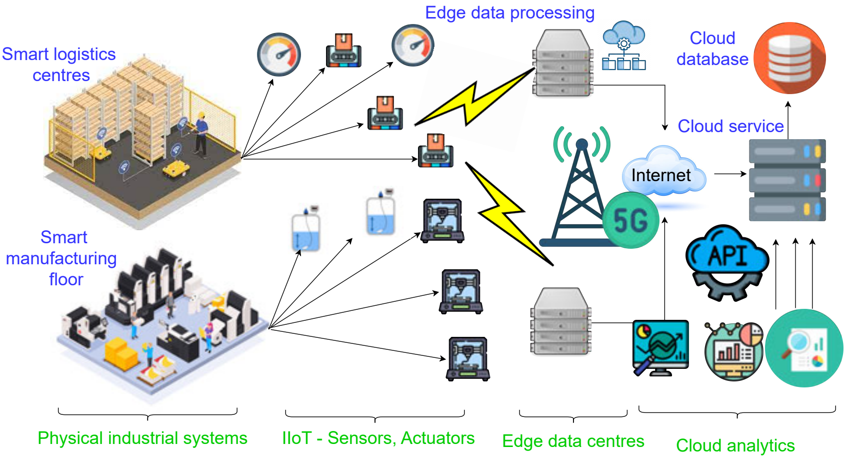

Fig. 2. IIoT system model in 5G networks.

2.2 Towards industrial internet of things from the internet of things

2.2.1 Evolution of the industrial internet of things

The 4th Industrial Revolution redefines the manufacturing paradigm with enhanced efficiency, safety, and increased profits for stakeholders. The diverse capabilities of IoT and associated communication technologies have unlocked the potential of IoT for the automation of industrial settings with real-time data collection, monitoring, and analysis. IIoT has emerged as a specialized type of IoT with a specific focus on industrial processes. IIoT focuses more on industrial applications, such as controlling manufacturing plants and smart supply chain management, than consumer applications, such as home automation and connected vehicles. Boyes et al.[28] explain the research articles that distinguish the IoT and IIoT, highlighting the core contribution of IIoT for manufacturing. Khan et al.[29] reflect the significance of IIoT towards a new vision of IoT to automate smart objects to sense, collect, process, and communicate real-time events in industrial systems. The authors highlighted the core objectives of IIoT, including operational efficiency, increased productivity, and better management of industrial assets and processes. Da et al. [30] present a comprehensive survey on current research of IoT, trends, and challenges with prominent IoT applications in the industries. Industrial stakeholders generally anticipate robust, efficient, and secured IoT systems to integrate manufacturing systems for better productivity and real-time data communication capabilities, such as IIoT.

2.2.2 Significant applications of industrial IoT

- Manufacturing: The applications of IIoT for manufacturing are diverse. These include the capability of remote monitoring and control of the manufacturing infrastructure[31, 32]. IIoT leverages data monitoring, quality control, and compliance establishment by integrating real-time data management [33] in manufacturing systems. IIoT enables connectivity with cloud [34] and edge computing [4] with extended computational capabilities for manufacturing.
- Healthcare: IIoT is transforming the healthcare infrastructure with vital capabilities with remote patient monitoring with cloud integration [35, 36]. IIoT can facilitate real-time patient data acquisition, processing, and management.
- Energy management: IIoT facilitates energy applications with different capabilities, including smart energy management [37], and energy trading[38], with machine learning-based energy management[39].
- Supply chain management: IIoT facilitates supply chain management applications with significant capabilities, including secured supply chain traceability [40]. IIoT improves the tracking, warehouse management, and customs clearing operations through automation with minimal human intervention.

2.2.3 Towards secured IIoT networks

Generally, in production-grade IoT systems, the components of the production line, such as actuators and sensors, are transformed into cyber-physical manufacturing systems [41, 42] connected to the cloud over the internet. Cyber-physical manufacturing systems have smart capabilities and inherent security threats [43]. With the evolution of IoT, the components of the production line, such as actuators and sensors, have been transformed into cyber-physical manufacturing systems [41, 42] connected to the cloud over the internet.

Panchal et al. [3] discuss the potential security threats to the IIoT, including DoS attacks, authentication attacks, and man-in-the-middle attacks, with some preventive measures. The authors also proposed IIoT attack taxonomy to mitigate the risks of attacks. Sengupta et al.[44] highlight the importance of preventing DDoS attacks and MiTM attacks in IIoT. The authors explore the challenges of the centralized IIoT architecture and highlight the potential of blockchain to address the identified challenges effectively. Tange et al. [45] highlight the security requirements of IIoT, including data privacy, authentication, and access control. The authors reflect on the potential of fog computing architecture to leverage the security of IIoT. Yu et al. [46] distinguish the IoT and IIoT security issues and comprehensively analyze industry-specific challenges. Tskinas and [47] present an analysis of threats in IIoT, including MitM attacks and DoS attacks. Overall, the literature highlights security as a vital requirement for IIoT. Based on the reviewed articles, potential security threats for IIoT can be summarized below. The threats have been decomposed further from the perspective of research questions formulated in this research in Section 4.3.

- Device spoofing attacks: In device spoofing attacks, the adversary impersonates the identity of a trusted device. The malicious IoT device may perform a physical operation or generate malicious data without being noticed by the stakeholders of the IoT system.
- Man-in-the-middle attacks: In MiTM attacks, the adversary operates between two parties of the IIoT communication channel and intercepts the communication between them with malicious data manipulation. The parties may not be aware of the forged data, and the adversary may monitor, inject, modify, or even corrupt the exchanged data. Furthermore, the adversary can spoof the identity and impersonate the exchanged malicious data.
- Targeted attacks: In targeted attacks, the attacker deliberately targets a critical service/system in the industrial application. In a targeted attack, the attacker gathers information and identifies the potential vulnerabilities that can be exploited. The attacker is driven by specific and well-defined objectives to target the attacking system. For example, the adaptive adversaries observe the IoT nodes with critical contributions to the network and attack/corrupt data on such nodes.
- Replay attacks: In replay attacks, the adversary repeats a particular message(s) to gain unauthorized access or attack the system. The adversary stores the data to formulate the replay message without the consent of the parties involved in the communication.
- DoS attacks: DoS attacks are malicious attempt that disrupts the function of IIoT systems as expected. The adversary who launches the DoS attack aims to render the IIoT system, network, or service unavailable to legitimate users or cause significant performance degradation in the system.
- Malicious data formulation: IIoT sensors formulate the data for processing, analysis, and storage. Maliciously formulated data affects the accuracy of the data utilization functions and overall reliability of the system.

ISO 27001 [48] defines security services for information systems. The security services include authentication, access control, data confidentiality, and availability. IEC62443[49] is a set of standards published by the International Electrotechnical Commission (IEC) with a comprehensive framework for ensuring the security of industrial automation and control systems, including IIoT systems. The IIC Security Framework [24]defines a specific set of security services for IIoT, including authentication, authorization, data confidentiality, and non-repudiation. National Institute of Standards and Technology (NIST) [50] defines identifying, protecting, and recovering as actions for incident response. The key security services identified to secure the IIoT networks in this research are as follows.

- IIoT node authentication: IIoT node authentication ensures that only the nodes with valid authentication credentials are trusted within the network.
- IIoT-Fog-Cloud channel data confidentiality: Ensuring data confidentiality in IIoT-Fog-Cloud channel ensures the adversaries cannot read and derive insights on the data transmitted over the untrusted channels, including the internet.
- IIoT-Fog-Cloud channel data integrity: Ensuring data integrity in IIoT-Fog-Cloud channel ensures the adversaries cannot modify the data transmitted over the untrusted channels, including the internet.
- Replay attack prevention: Replay attack prevention ensures the IoT nodes cannot repeatedly send the same messages for malicious purposes in industrial applications.
- Malicious IIoT node detection and off-boarding: The malicious IIoT nodes must be identified and flagged as untrusted based on the behaviour on the network.
- DoS/DDoS attack detection prevention for the network slice broker: DoS/DDoS attacks in the network must be detected and prevented to ensure the network slice broker's persistent service delivery for the network's legitimate users.
- Reputation score and consensus for evaluating the malicious data: Reputation score is a potential indicator of the trust level and reliability of a blockchain node in the network. The higher reputation of blockchain nodes must be increased in block mining contribution.
- Defending high-reputation blockchain nodes from adaptive adversaries: The reputation score must be hidden from the adversaries to eliminate targetting the high-reputation mining nodes from the adversaries who specifically target them to attack.

Efficiently securing IIoT using decentralized technologies is the utmost objective of this research. Establishing the security of IIoT systems includes actions to preserve fundamental security properties of the system.

The NIST Cyber Security Framework [51] proposes five core functions: identify cyber security risks, protect from cyber threats, detect cyber security events, respond to cyber security incidents, and recover functions and operations exposed to an attack. Table 1 provides an overview of the proposed research from the perspective of the NIST cyber security framework. Section 4.3 decomposes the identified threats and limitations for a clearer interpretation of the research.

2.3 Definitions of important terms used in research

2.3.1 *Efficiency*

The term efficiency defines the capability to accomplish a specific task with minimum resource utilization. From the perspective of securing the IIoT networks, efficiency is relevant in different scenarios[52]. Computation efficiency is important as the IIoT networks comprise heterogeneous nodes with different computational capabilities. Computationally efficient services enable low-computational powered IIoT networks to compute security-related functions. Efficiency in bandwidth and storage are preliminary requirements for IIoT as production-grade IIoT networks consist of many nodes connected to physical functions. Services with efficient bandwidth and storage incur as minimal impact on the network and storage services such as databases. Efficiency in time reflects the minimal end-to-end process completion time. Energy efficiency is important to ensure the cost-effective operation of IIoT networks with minimal energy consumption. The energy efficient[53] IoT survives with limited power for a longer time and ensures cost-effective operation.

2.3.2 *Malicious adversaries*

An entity in the IIoT network is considered an adversary when it deliberately behaves to fundamentally compromise the security features of the network[54]. The adversary can be either a person, a software program, or a device in the network. The malicious adversaries are further classified into subcategories depending on their objectives and behaviour. For example, the slowly adaptive adversaries observe the system and attack the members of the network that commit a significantly higher contribution.

2.3.3 *Decentralization*

Decentralization refers to a specific service or data in more than one instance. The service consumers can invoke multiple instances of services depending on the conditions. Decentralized data ensures the existence of multiple copies of data instances. However, the consistency of service and data is important to ensure real decentralization features.

Table 1. A high-level overview of the research in NIST cyber security framework.

Function	RQ	Solution in the research	Article	Remarks
Identify	RQ1,RQ2, RQ3	Technical review on the state of art	All	The research reflects the potential threats of IIoT in the literature review with the potential limitations of the state of art.
Protect	RQ1,RQ2, RQ3	IoT node authentication, protect NSB from DoS/DDoS attacks, protect the ledger records by ensuring anonymity and unlinkability, protect the high-reputation blockchain nodes from adaptive adversaries	All	The research contributes with decentralized security services on protecting the IIoT networks
Detect	RQ1,RQ2, RQ3	Smart contract-based threat scoring with IDS integration, profile-based detection of malicious tenants and resource providers, Reputation score-based detection of malicious IoT nodes	Paper I, Paper III, Paper VI	The smart contracts operate as decentralized services to detect the malicious attempts and proceed on response in realtime
Respond	RQ1,RQ2, RQ3	Smart contract-based revocation of IoT certificate upon exceeding the threshold value of the threat score, preventing the malicious IoT tenants sending slice requests to the NSB, disabling lower reputation score blockchain nodes to mine the blocks	Paper I, Paper III, Paper VI	The results reflect the resistance to the attacks through simulation
Recover		Distributed ledger integration	All	The distributed ledger is redundant data storage with cryptographically-preserved multiple instances on the ledger.

2.3.4 Trust

Trust in IIoT networks refers to the reliability and confidence of a node, service, or communication channel. A trusted IIoT node ensures that the data exchanged or generated from the IIoT node is reliable and not manipulated by malicious adversaries. The trusted communication channel ensures the exchanged data is secured and the anticipated security requirements are preserved. The IIoT trust can be further decomposed into different types such as device trust, connection trust, system trust, and processing trust[55]. Reputation scoring is [56] one potential approach for numerical evaluation of the trust. Overall, trust indicates reliability, fairness and attack resistance[55] in IIoT networks.

2.3.5 Anonymity and unlinkability

Anonymity and unlinkability ensure IoT authentication-related transaction data, which is visible to the curious parties, is not linked directly to specific individuals or devices that could formulate identity or scale-related insights from the available data. Anonymity and unlikability protect the privacy of IoT nodes and prevent unauthorized access to their identity information. In the process of implementing anonymity and unlinkability, collaborative systems such as blockchain need to preserve the privacy of sensitive information to safeguard the members' confidence on the system.

2.4 Network slicing and slice brokering in IIoT

2.4.1 5G and beyond networks for IIoT connectivity

5G and beyond mobile networks are the most promising connectivity enablers for the future IIoT. The distinguishing types of communication in 5G and beyond networks are,

- Enhanced Mobile Broadband (eMBB): eMBB ensures high data rates, enabling faster data transfer than the earlier generations of mobile networks. Industrial applications such as remote monitoring, video surveillance, and AR require faster data transfer speed to ensure uninterrupted data streaming.
- Ultra-Reliable Low-Latency Communications (URLLC): -URLLC ensures low latency and high reliability for mission-critical industrial applications, such as remote surgery or automated vehicular networks. URLLC applies to IIoT applications requiring real-time low-latency data transfer and highly reliable connectivity for mission-critical infrastructure with IIoT.

– Massive Machine-Type Communications (mMTC): -mMTC is a service that ensures connectivity for many low-power, low-data-rate devices, such as sensors or meters connected to the industrial infrastructure. The IIoT applications that require many devices with a scale of one million per square kilometre are significant applications of mMTC.

The IIoT connectivity of 5G and beyond networks relies on physical resources, including the radio spectrum, network servers, and edge computing infrastructure. Mobile Network Operators (MNO) and local 5G Operators deliver the RAN, core network services in a service-based architecture to the IIoT tenants[57]. The Mobile Network Operators (MNOs) and local 5G Operators contribute to the connectivity of IIoT in two distinct approaches.

MNOs provide a wide coverage of connectivity using the extensive network infrastructure, enabling seamless connectivity for broad-scale IIoT deployments across vast geographic regions. Local 5G operators deploy specialized, private, and standalone 5G network instances within a specific and limited geographic region. The local 5G networks are tailored to specific industrial settings with customized service features and stringent security needs. The local 5G operators ideally facilitate connectivity for factories with connected manufacturing equipment in a limited region [58]. The local 5G operators provide edge computing processing power for the decentralized network infrastructure, which is closer to the physical and operational environment of the IIoT.

Improved efficiency, security, and the distinguishing features of 5G, such as network slicing, enhance and enable diversified connectivity features for the industry verticals. Hassan et al. [59] reflect the insights of 5G network architecture and the significance of emerging technologies for potential applications in IIoT, including edge computing and network slicing. Abbas et al. [60] highlight the potential of eMBB, URLLC, and mMTC to deliver reliable and efficient communication for IIoT applications. Hussain et al. [61] highlight the potential of 5G networks to improve data rates, energy efficiency, and reliability of IIoT. Islam et al.[62] emphasize the significance of security principles, including privacy, integrity, and availability in the IIoT. The authors also highlighted the requirement of authentication, confidentiality, and data protection and the potential of emerging technologies, such as blockchain, for securing the IIoT. Jiang et al.[63] discuss the security challenges and potential solutions in 5G-enabled IIoT. The authors propose secured key management, data storage, and communication protocols to enable secure communication and data confidentiality on the IIoT. The authors reflect on the importance of security standards and regulations for IIoT systems. In [64], the authors highlight the requirement of low latency, high reliability, and massive connectivity in IIoT systems and reflect the security, privacy, and interoperability challenges. The proposed solutions include emerging technologies, network slicing, and edge computing.

However, both MNO and local 5G operators share similar resources in the context of connectivity for IIoT. MNOs and local 5G operators rely on acquiring and managing spectrum resources to the IIoT. MNOs and local 5G operators depend on security techniques such as authentication, encryption, and firewalls. Furthermore, the MNOs and local 5G operators use network slicing to cater to individualized services for different IIoT tenants. In this thesis's research contribution on efficient and secured network slice brokering, both MNOs and local 5G operators are considered from a generalized perspective as resource providers to broaden the application potential of the proposed work.

2.4.2 Network slicing and network slice brokering

5G mobile networks are designed with the vision to accommodate the diverse service requirements for different stakeholders (e.g. Mobile Virtual Network Operators, Over The Top service providers, and industry verticals) in the telecommunication ecosystem [65]. Thus, it is required to customize and partition the same 5G physical infrastructure between these stakeholders to satisfy their diverse service requirements. In this context, Network Slicing (NS) [66] has emerged as one of the building blocks of the 5G and beyond 5G networks. 5G network slicing allows the on-demand creation of multiple End-to-End (E2E) logical networks over a common physical (mobile network) infrastructure. Network slicing enhances the overall user experience and enables the successful deployment of various technologies like 5G, IoT, and edge computing. Following the trends observed in the 5G era, 6G is envisioned to intensively use sophisticated and secure slicing for complex multi-tenant multi-operator scenarios.

Kuklinski et al. [67] emphasize the potential business models of network slicing in single-domain and multi-domain network slicing. The authors also highlighted the limitations of the ETSI(European Telecommunications Standards Institute) NFV MANO(Network Functions Virtualization Management and Orchestration) architecture in a multi-provider environment and proposed modifications.

Efficient network sharing is one of the most vital requirements in future telecommunication in terms of consumer service values and profitability of resource providers (RPs), including mobile network operators (MNOs) [68]. Slicing allows the realization of a multi-tenancy paradigm where multiple network tenants can simultaneously access the shared computing, storage, and networking resources an infrastructure provider offers. Network tenants can be an industry vertical, a Mobile Virtual Network Operator

(MVNO), or an Over-The-Top (OTT) service provider. A network slice broker is an entity that facilitates the formation of new slices based on consumers' requirements. Slicing also allows infrastructure providers to virtualize and trade their resources dynamically to network tenants, thereby allowing better business models with optimal slices that provide lower prices to the tenant and a higher profit to the MNOs. Kuklinski et al. [67] emphasize the potential business model of single-domain and multi-domain network slicing. The authors also highlighted the limitations of the ETSI NFV MANO architecture in a multi-provider environment and proposed modifications. Wijethillake and Liyanage [66] emphasize the role of network slicing in IoT with significant technical challenges.

In 5G, network slice brokering is introduced as a new business model for dynamic network sharing wherein a logically centralized entity named the slice broker governs the resource trading between infrastructure providers at one end and multiple network tenants at the other end [69]. However, apart from facilitating on-demand resource allocation, a slice broker performs admission control based on traffic monitoring and forecasting and mobility management based on a global network view. It configures Radio Access Network (RAN) schedulers to support multi-tenancy use cases. As defined in [69], a 5G network slice broker is co-located with the Master Operator-Network Manager (MO-NM), which monitors and controls the shared RAN and interacts with the Sharing Operator-Network Manager (SO-NM), which provides feedback. In the multi-operator and multi-tenant IIoT scenarios that are envisioned in 5G and beyond, it is important to enable real-time network slice brokering service with improved latency and advanced security, which has been investigated in this research.

2.4.3 DoS and DDoS attacks in slice brokering

Though NSBs offer numerous advantages, nevertheless, it is vulnerable for new security limitations and issues that can hinder the deployment of network slices. In particular, the issues corresponding to DoS and DDoS attacks are envisioned to be of high importance. In DoS/DDoS attacks, the compromised network tenants(s) and/or the compromised MNOs maliciously overwhelm an NSB entity to either slow or sabotage its work. As a result, there can be adverse effects like delaying the creation of genuine and legitimate network slices, inefficient utilization of computational and network resources, glitches in SLA compliance, and diminishing trust in the network and associated services. Hence, DoS/DDoS attacks can be a significant impediment to deploying NSB services for network automation, so designing a mechanism to mitigate such attacks on NSBs is essential.

Though NSBs offer numerous advantages, nevertheless, it is vulnerable to new security limitations and issues that can hinder the deployment of network slices. In particular, the issues corresponding to DoS and DDoS attacks are envisioned to be of high importance. In DoS/DDoS attack, the compromised network tenants(s) and/or the compromised Mobile Network Operators (MNOs) maliciously overwhelm NSB entity with the intention to either slow down its working or sabotage it. As a result, there can be adverse effects such as delaying the creation of genuine and legitimate network slices, inefficient utilization of computational and network resources, glitches in SLA compliance, and diminishing the trust in the network and associated services. Hence, DoS/DDoS attacks can be a significant impediment to the deployment of NSB service towards network automation so it is essential to design a mechanism to mitigate such attacks on NSBs.

Cunha et al. [70] presents a comprehensive review on security challenges in network slicing and highlight the problem of DoS attacks in network slicing. On the one hand, numerous studies such as [71] and [72] aim to secure network slices against DoS attacks. On the other hand, there are works such as [73, 74, 75] that deal with DoS/DDoS attacks on 5G networks. However, none of them discuss about DoS/DDoS attacks on NSB entities. Blockchain is a well-known Distributed Ledger Technology (DLT), which has a huge potential to be used as a supporting technology for 5G and 6G networks [76, 77, 78].

The role of 5G NSBs is introduced as a novel business model to enable the dynamic interoperability and resource trading requirements of market players such as infrastructure providers, consumers, and MNOs in trading the network and computational resources [69]. An NSB acts as a mediator between the MNO and the network tenants. Based on the resource requests received from the tenants, the NSB creates a network slice template and broadcasts it to prospective MNOs. After receiving the offers (i.e., the price list for available resources) from the MNOs, the NSB selects the best matching offer for the given request and provides the network slice to the tenants. According to the architecture of the NSB, there are mainly two contact points (i.e., tenants and MNOs) from where DoS attacks can be mounted on the NSB.

2.5 Reliable IIoT data formulation

The Internet of Things (IoT) empowers physical objects with the capabilities of intelligent entities and internet connectivity. IoT application domains exist in two forms: sensing applications and industrial automation. In sensing applications, massive data is streamed via the cloud and edge computational infrastructure for different enterprise applications, including data analytics, machine learning, and data sharing. The augmentation of IoT with sensors and actuators results in intelligent automation in various industrial domains, including healthcare, smart city, energy management, logistics, construction, and environmental protection. The application contexts of IoT data include descriptive analytics based on real-time data, predictive analytics to formulate future predictions based on past data, and the training of machine learning for different application contexts. Reliability in IoT data is important to ensure the successful working of IoT applications[79].

2.5.1 Domain-specific data validation and computation on the encrypted data

The generated data from the sensor network forms the baseline to train machine learning models, forecasting, diagnosis, and insight derivation for critical enterprise applications. Manipulating sensor data by malicious parties affects the data utilization function, potentially yielding incorrect results. Thus, industrial context-specific data validation frameworks enhance the reliability of data by the definition of features to distinguish malicious data from non-malicious data. Alduais [80] presented several frameworks, including the Euclidean distance and a distance matrix, to determine the validity of data emitted in wireless sensor networks. Hussain et al. [81] presented a medical IoT sensor data validation framework based on the numerical range and arrival time profiles of IoT data. Avcko et al.[82] highlighted a means of meteorological data validation for the IoT in Industry 4.0. Sandor et al. [83] proposed an abnormal sensor behaviour detection mechanism based on Apriori knowledge. These validation frameworks are algorithms that can eventually be implementable as a computer program.

Encryption that supports computation on encrypted data advances the security of IoT applications with improved privacy. The computational capability of the encrypted data facilitates the derivation of essential insights from the encrypted data without revealing individual values generated from the sensors for potential applications, such as healthcare sensors that formulate cloud databases of human body parameters. Revealing the individual patients' body parameters is a significant compliance breach of laws, such as HIPAA. In addition, IoT-integrated smart energy is a prominent industrial application for regional power consumption forecasting. It is a privacy breach if individual residents' power consumption statistics are revealed to other parties. Secure multi-party computation is one of the most prominent computation applications for privacy-preserved data. Deng et al. [84] proposed identity-based encryption for a privacy-preserved data-sharing scheme for IoT. Tso et al. [85] proposed a privacy-preserved data communication framework for IoT connectivity to the cloud with secure multi-party computation. Sharma et al. [86] proposed a privacy-preserved healthcare data analysis framework. Li et al. [87] proposed a privacy-preserved diagnosis framework based on homomorphic encryption. Guan et al. [88] proposed a privacy-preserved data aggregation scheme for IoT. Most techniques are algorithms with standard encryption mechanisms that can be encoded as computer programs. However, the different types of sensor data encryption techniques are resource-intensive functions. Encryption on the sensor itself impacts the sensor's battery life, and encryption on the cloud has emerged as a central point of failure with limited scalability. Delivering the encryption function to the edge layer is a significant design decision for scalability-focused IoT networks. However, the above applications rely on valid, trusted, and reliable data to yield accurate results based on the input data. Therefore, data reliability is important to utilize the data with guaranteed accuracy.

2.6 Authentication and encryption techniques in IIoT

Authentication and encryption are two important techniques to secure the IIoT. More specifically, authentication of IIoT devices, entities, and services prevents unauthorized access by adversaries to IIoT networks and sensitive information of industrial applications. Authentication of the communication, including the messages exchanged at the communication endpoints, ensures the resistance to MitM attacks that intercept and manipulate the messages of industrial processes. Encryption of IIoT data ensures the confidentiality of messages and exchanged data. Encryption prevents IIoT data from being exchanged between communication endpoints and stored in data storages inaccessible to adversaries. This research includes a significant contribution to facilitating IIoT authentication and encryption efficiently. This section explains the cryptographic protocols and principles for the authentication and encryption of IIoT.

2.6.1 Elliptic curve cryptography(ECC) and the elliptic curve integrated encryption scheme (ECIES)

Most lightweight public key-based operations are realized with Elliptic Curve Cryptography (ECC), defined on the algebraic structure of elliptic curves (ECs) over finite fields F_p generated by a generator point G. The two major operations in ECC are EC point addition $P_1 + P_2$ and EC point multiplication rP with a scalar r. The security of ECC relies on two hard computational problems, the Elliptic Curve Discrete Logarithm Problem (ECDLP) and the Elliptic Curve Diffie Hellman Problem (ECDHP).

ECIES is a computationally efficient encryption algorithm when compared with the state of art algorithms used for encryption on IIoT. For encrypting a message M to the receiver with a public key Q_R, the sender generates a random value r and computes $A = rG$. A symmetric session key K is now defined by $K = rQ_R$, which can also be derived by the receiver $K = d_R A = rQ_R$, who knows the private key d_R for which $Q_R = d_R G$. ECIES has been utilized in RQ1 in this research.

2.6.2 The Schnorr signature scheme

To sign a message M, a user with a key pair $(d_n, Q_n = d_n G)$ chooses a random value r and computes $R = rG$. Next, it derives $h = H(M,R)$, where $H(.)$ is a one-way collision-resistant hash function. The signature is then defined by $s = r - hd_n$. The user makes the message M, together with R, s public. Any other party can now verify that the message M is signed by the user with public key Q_n, by checking the equality $sG = R - H(M,R)Q_n$. The research also denoted this process by

$$M_{s_{d_n}} = \{M, R, s\}, \tag{1}$$

for the signature generation and $M_{s_{Q_n}} = \{Y, N\}$ for the signature verification. Schonrr signature scheme has been utilized in RQ1 of this research.

2.6.3 Elliptic curve non-interactive zero-knowledge proof based on Schnorr signatures

In this proof, it is required to assume that the prover and the verifier agree on the EC, the generator G and one additional EC point P. The goal of the proof is to convince the verifier that the prover possesses b, given $B = bG$ and without sharing additional information on b.

To this end, the prover generates a random value r and computes $A = rG$. Next it defines $c = H(xP, rP, A)$ and $s = r + cx$. The proof consists of the set of values $\{s, xP, rP, A\}$.

Upon arrival of the proof, the verifier first computes $c = H(xP, rP, A)$ and checks if both equalities $sG = A + cB$ and $sP = rP + cxP$ are valid. If so, the verifier is convinced.

EC-NIZKP has been utilized in the RQ1 of this research.

2.6.4 Encrypted IoT data formulation

Encryption that supports the computation of encrypted data advances the security of IoT applications with improved privacy. The computational capability of the encrypted data facilitates the derivation of essential insights from the encrypted data without revealing individual values generated from the sensors for potential applications, such as healthcare sensors that formulate cloud databases of human body parameters. Revealing the individual patients' body parameters is a significant breach of compliance with statutes, such as HIPAA. In addition, IoT-integrated smart energy is a prominent industrial application for regional power consumption forecasting. It is a privacy breach if individual residents' power consumption statistics are revealed to other parties. Secure multi-party computation is one of the most prominent applications of computation using privacy-preserved data. Deng et al. [84] proposed an identity-based encryption method for a privacy-preserved data-sharing scheme for IoT. Tso et al. [85] proposed a privacy-preserved data communication framework for IoT connectivity to the cloud with secure multi-party computation. Sharma et al. [86] proposed a privacy-preserved healthcare data analysis framework. Li et al. [87] proposed a privacy-preserved diagnosis framework based on homomorphic encryption. Guan et al. [88] proposed a privacy-preserved data aggregation scheme for IoT. Most techniques are algorithms with standard encryption mechanisms that can be encoded as computer programs. However, the different types of sensor data encryption techniques that utilize cryptographic functions are challenging to implement on the sensors due to the limited computing resources available on the sensors. Encryption on the sensor itself impacts the battery life of the sensor, and the encryption on the cloud emerged as a central point of failure with limited scalability. Delivering the encryption function to the edge layer is a prudent design decision for scalability-focused IoT networks.

2.7 Bulletproof mechanisms

Bulletproof mechanisms enable privacy-preserved and bandwidth-efficient zero-knowledge proof. In general, zero-knowledge proofs include proof generation and verification, which consist of multiple steps between the prover and verifier. Scalability is a primary consideration of IIoT networks, and this research focuses on bandwidth and energy efficiency for securing IoT networks using ZKP. This section includes an overview of the principles of Bulletroofs that are utilized in the study for reputation score verification in the proposed novel consensus protocol for RQ3. BulletProof mechanism was used in

RQ3 for energy and bandwidth-efficient reputation score verification with preserved privacy.

2.7.1 Pedersen commitment

The Pedersen commitment scheme is an essential building block in a Zero-Knowledge Proof (ZKP) that enables proof of knowledge of a value to the verifier without revealing the value. The Pedersen commitment scheme is based on Elliptic Curve Cryptography (ECC). The Pedersen commitment proof consists of initialization, commitment, and opening phases.

Initialization phase includes the selection of an Elliptic Curve $E(F_p)$ with generators G and H, and order q. The public parameters are (G, H, q).

Commitment phase includes the prover's selection of a blinding factor r and generation of the commitment for the message m as,

$$Comm(m) = rG + mH.$$

Proof phase includes sending the blinding factor and the actual value as a tuple (r, C) and the verifier checks whether the received commitment is equal. The benefit of a Pedersen commitment is its additive homomorphism. As example, assume that the Pedersen commitments for m_1 and m_2 are defined as,

$$\begin{aligned} Comm(m_1) &= r_1G + m_1H = C_1, \\ Comm(m_2) &= r_2G + m_2H = C_2. \end{aligned}$$

$C_1 + C_2$ forms a curve point C_3 such that C_3 is the Pedersen commitment for $m_3 = m_1 + m_2$ with the blinding factor $r_3 = r_1 + r_2$. Here, all values are defined as modulus p with,

$$\begin{aligned} C_3 = Comm(m_1 + m_2) &= Comm(m_1) + Comm(m_2), \\ C_3 &= (r_1 + r_2)G + (m_1 + m_2)H. \end{aligned}$$

2.7.2 Range proofs using Bulletproof

Bulletproof [89] is a short, non-interactive ZKP that does not require a trusted setup. In Bulletproof, the public validation of a number $m \in [0, 2^n]$ is possible without revealing the actual numbers. Bulletproofs validate whether a difference between two numbers $m_1 - m_2$, which is presented as a Pedersen commitment, is within the range $[0, 2^n]$

(eg. $n = 64$) If $m_1 \geq m_2$,$(m_1 - m_2) \in [0, 2^n]$ and if $m_1 < m_2$ the difference cannot be represented as a number between $[0, 2^{64}]$ due to the overflow of bits In this proof, the original values m_1 and m_2 are represented as Pedersen commitments to preserve privacy.

2.8 Blockchain as a more robust and decentralized service enabler

The advancements in IoT and the arrival of 5G have popularized the development of 5G-enabled IoT applications. Such applications pose stringent requirements such as high capacity, assured privacy & security, scalability of heterogeneous applications, ultra-low latency, optimized use of network resources, efficient energy management and low operating expenditure (OpEx)[90]. Even though the security architectures that are currently being used for mobile networks and generic IoT systems match the required expectations, they are in principle centralized [91], [92], [93]. Using such centralized security solutions for 5G and 5G-enabled-IoT applications will lead to various impediments like increased cost due to inherent heterogeneity, complex and static security management procedures, over-utilization of network resources, creation of bottleneck in the network, single point-of-failures, a high OpEx, etc. Thus, continuing to use centralized security solutions for 5G and IoT-driven applications will not only struggle to meet the demands but will also adversely affect the projected visions of 5G and IoT. Lately, blockchain technology and in general, distributed ledger technology have gained momentum and have been embraced by industry and research communities across the globe.

It is important to consider the attack potential of the blockchain. Attacking a blockchain with a malicious chain is possible by dominating the consensus process. In this scenario, an entity or group of entities deliberately reach the control conditions required for block mining. With this control, the adversaries can create their parallel blockchain (the malicious chain) and attempt to outpace the legitimate blockchain by adding new blocks, which is known as a forking attack[94]. If successful, the adversaries can rewrite transaction history or carry out other malicious actions. However, this entire attack effort is computationally challenging, with extensive effort for consensus condition generation, cryptographic signature forging and approval, which motivated the incorporation of blockchain in this research. In addition, the distinguishing features of blockchain facilitate IoT security services, including trust[95], which has motivated this research to incorporate blockchain for securing IIoT. This research utilizes the blockchain and distributed ledger technologies to deploy the security service functions on the fog infrastructure layer to efficiently deliver the security services for the IIoT.

2.8.1 Functional overview of blockchain

The blockchain is a decentralized, immutable ledger which is composed of a cryptographically linked chain of blocked records. The collections of records are called blocks, usually called transactions or events. The decentralized ledger is shared within all contributory members in the blockchain network [96]. Transactions are added to the ledger upon a verification and agreement process between the parties in the blockchain. The cryptographic link is the backbone of the blockchain. The important keywords associated with blockchain are the ***decentralization***, ***immutability*** and ***cryptographic link***. These keywords are explained below.

Decentralization: The decentralization reflects the transaction processing(execute a function, store and retrieve data) capability of blockchain-based smart contracts without a single point of failure. The ledger is available on each node, and in contrast with centralized database management systems [97], access to the data does not depend on a centralized service.

Immutability: The records in the ledger are immutable once logged [98] An attempt to forge a ledger record on a particular block will disqualify it and fail the data integrity of the entire blockchain. The immutability of the ledger is ensured using cryptographic techniques such as hashing and digital signatures. The alterations of a ledger is a computationally expensive task.

Cryptographic link: A cryptographic link is the backbone of trust of the entire blockchain [99] The immutability of a blockchain is achieved through the cryptographic link established with hashing and digital signatures [100]. Neither a transaction or block can be altered since it requires altering all subsequent blocks.

Figure 3 reflects the transaction workflow of a blockchain network. A brief description of the common steps of blockchain are as follows.

- *Step 1*: The blockchain node receives the events to be included in the blockchain. In industrial applications, the deployed APIs of the blockchain integrate the blockchain as a service with IIoT systems to capture external events with relevant data elements.
- *Step 2*: The blockchain node converts the event into a form of transaction by extracting each data element received from the external service.
- *Step 3* : The blockchain node waits until the node is qualified for mining. The node holds the transactions in the unmined transaction pool.
- *Step 4*: When the node has reached the qualifying condition for mining, the node generates the relevant parameters of new block. These values include the hash values of the Merkle tree, block header, and digital signatures of the transactions. The block will be disseminated in the network for approval.

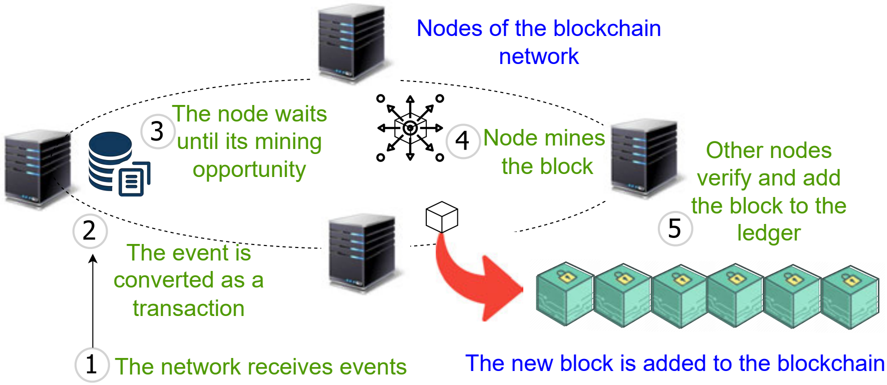
Nodes of the blockchain network
3 The node waits until its mining opportunity
4 Node mines the block
Other nodes verify and add the block to the ledger
5
2
The event is converted as a transaction
1 The network receives events
The new block is added to the blockchain

Fig. 3. Blockchain transaction workflow.

- *Step 5* : Other nodes verify the conditions for mining node election, verify the digital signatures and add the new block into the chain.

2.8.2 Overview of the consensus protocols

The consensus protocol defines the conditions to achieve consistency among the distributed nodes. The validation and confirmation of the transactions are preceded by collective decisions of the members in the blockchain network to ensure a non-tampered and consistent ledger [101]. The consensus protocol includes the condition to finalize the transaction, defined as transaction finality [102]. It is important to consider the requirements of the blockchain network and determine the consensus protocol. The mining criteria of the consensus processes are classified as follows.

- **Proof of Work (PoW)**: PoW-based consensus protocols enable all the mining nodes to compete on a puzzle to be qualified for adding the blocks to the blockchain. Solving a puzzle requires significant computational power. The winning node that solves the puzzle will be elected for mining. Bitcoin [16] is the most prominent example of PoW consensus protocol. However, consensus protocols like PoW consume a significant amount of energy to be qualified for mining.
- **Proof of Stake (PoS)**: PoS-based consensus protocols select the winning mining node based on the ownership of cryptocurrency. Etherum [103] is a well-known example of PoS consensus protocol.
- **Practical Byzantine Fault Tolerant Consensus Protocols (PBFT)** In PBFT, the members of the blockchain networks are limited to a selected group. The members

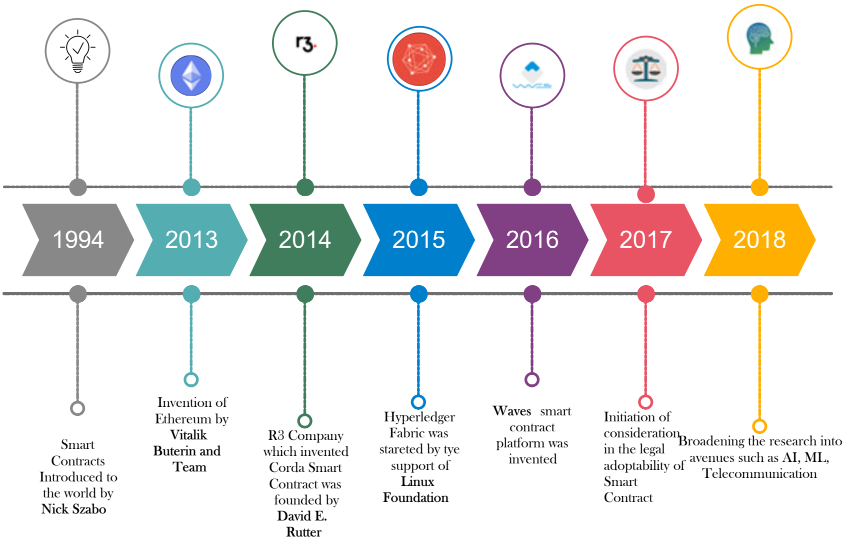
1994
2013
2014
2015
2016
2017
2018
Smart Contracts Introduced to the world by Nick Szabo
Invention of Ethereum by Vitalik Buterin and Team
R3 Company which invented Corda Smart Contract was founded by David E. Rutter
Hyperledger Fabric was stareted by tye support of Linux Foundation
Waves smart contract platform was invented
Initiation of consideration in the legal adoptability of Smart Contract
Broadening the research into avenues such as AI, ML, Telecommunication

Fig. 4. Smart contract evolution timeline (Reprinted, with permission, from [106], 2021 © IEEE).

vote for a new block that is being proposed by the mining node and the block approval requires a predefined number of votes. The blockchain network is fault tolerant even though a certain number of members in the network are malicious. Hyperledger [104] utilizes a variant of PBFT consensus protocol.

– **Index-based consensus protocols** Index-based consensus protocols maintain the reputation of the individual nodes based on certain criteria. The nodes with high reputations are elected for mining. Proof of Familiarity [105] is a significant example that utilizes experience on a particular disease as an index of collaborative partners of the blockchain network for medical decision-making. However, the index-based consensus protocols do not resist against the attacks launched by slowly adaptive adversaries that target the high-reputation blockchain nodes.

2.8.3 Blockchain-based smart contracts as foundational elements for the research

Nick Szabo first introduced the concept of smart contracts. Ethereum [103] is one of the most prominent smart contract platforms with multitudinous applications in different contexts. Initially, smart contracts were targeted only for financial applications such as

ERC20 tokens [107]. Over time, the invention of smart contract platforms diversified due to various industrial requirements [108].

Figure 4 illustrates the important milestones in the historical evolution of blockchain-based smart contracts. The introduction of the concept of smart contracts was by Nick Szabo to the world in 1994 was the birth of smart contracts. The invention of Ethereum is one of the most important leaps in smart contract history. The public Ethereum blockchain allowed users to onboard and deploy smart contract applications in public blockchains. Ethereum was primarily targeted for currency exchange at the beginning. The Hyperledger Fabric project was initiated in collaboration with the Linux Foundation. The direction of the Hyperledger Fabric has deviated from Ethereum's since Hyperledger was intended as an enterprise blockchain. Many platforms are being developed target enterprise requirements. The next generation of research is highly focused on the position of smart contracts as an emerging research topic in computer science.

Smart contracts are self-enforcing and self-executing programs which actuate the terms and conditions of a particular agreement using software codes and computational infrastructure. Smart contracts are decentralized programs that extend the use of the underlying blockchain network [109]. The program is immutable and is cryptographically verified to ensure its trustworthiness.

Some features of smart contracts are inherited from the underlying blockchain technology. These features enable the deployment of smart contracts across diverse domains[110]. Generally speaking, smart contracts are executed in peer-to-peer mode without the intervention of a centralized third party. They provide service availability without any centralized dependency and they allow automated transaction execution when pre-defined conditions are met[111]. Below the research details the key features of blockchain-based smart contracts.

- **Elimination of Trusted Third Party and Autonomous Execution**: The most significant advantage of blockchain-based smart contracts is decentralization [112]. The requirement of trusted intermediaries such as brokers, agents or service providers can be replaced with smart contracts. Eliminating a trusted third party will reduce the transaction costs and authority imposed by centralized entities. One of the most significant examples is cryptocurrency which embraced smart contracts to alter the role of trusted third parties such as central banks [113]. Centralized third parties impose high transaction costs and behave as the ultimate governing bodies. The users need to adhere to the regulations imposed by the centralized authorities.

  In contrast, smart contracts provide the agreement procedure to be defined by the participants themselves, maximizing democracy [114]. The participants define the rules and regulations for the smart contract establishment and deploy them upon mutual agreement. The programmed condition and flow of events are supposed to execute once the blockchain reaches a specific pre-defined state. The specific state will be defined in the smart contract upon the agreement of all parties in the blockchain network. This state can be any condition, such as a specific balance of wallet funds a specific time-bound, etc. The execution is then automatic without intervening a centralized third party. The service availability is guaranteed since the operation does not rely on a centralized third party and executes peer-to-peer. The autonomous execution as per the conditions, ensures operation accuracy without human error or even biased actions. Therefore, the smart contract is a promising solution for most applications which require alternatives without trusted third parties.

- **Forge Resistance and Immutability**: The integrity of the transaction records in the distributed ledger is verified with digital signatures [115]. Furthermore, the individual transactions are verified and approved before appending to the ledger. The ever-growing ledger consists of approved transactions which are immutable. The alteration cannot be committed by an individual. Smart contract codes deployed on the blockchain are immutable. The code can be deployed on each node using various techniques, such as an executable enclosed in the container. The smart contract code is tamper-evident, and the tampered smart contracts cannot be executed. However, smart contracts can be updated if required upon the agreement of nodes in the blockchain network. Therefore, all parties in the blockchain network can trust the smart contract and trust that the executed code contains the logic disclosed to and agreed by each member of the blockchain network.
- **Transparency**: Transparency [116] is one of the significant distinguishing features inherited in smart contracts from blockchain [117]. The transparency of the smart contract is twofold. Firstly, the code defined in smart contracts is transparent to intervening parties as well as to the public. Secondly, the set of transactions included in the blocks is also transparent to the public. Hence, the intervening parties of the blockchain network can trust the logic and transactions in the blockchain network [118]. In a more concrete example, if the smart contract logic defined by a governing authority who is a participant of blockchain network [119]. The smart contract executes the particular operation, and the logic can be regarded as trusted and unbiased since the execution program, which is encoded as a smart contract, is publicly visible. Furthermore, the transaction added to the ledger is also publicly visible to ensure trust [120]. In contrast, the centralized service architecture is not transparent and is prone to vulnerabilities such as man-in-the-middle attacks. Centralized databases are also vulnerable and impossible to trace if any modification has occurred to the data. The

smart contract code transparency [121] ensures members of the blockchain ecosystem publicly verify its execution correctness.

Overall, the self-executing, code-based agreements can facilitate secure and trustless interactions between IIoT devices, including transparency and non-repudiation[122], enforcing predetermined rules and conditions without the need for intermediaries. This not only reduces the risk of human error and fraud but also enhances the integrity of data exchanges and the overall security of IIoT systems with guaranteed non-repudiation[123]. Additionally, the decentralized nature of blockchain platforms, where smart contracts are deployed, further strengthens security by distributing the control and verification of transactions across a network, making it exceedingly challenging for malicious actors to compromise the system. As IIoT applications continue to grow in complexity and scale, smart contracts offer a promising avenue for enhancing the security and reliability of IIoT systems. These features were the foundational aspects that motivated the applicability of smart contracts as a decentralized service enabler for the security algorithms to be deployed for efficiency anticipations in IIoT.

2.8.4 Operating modes of blockchain

Blockchain networks consist of multiple members; the events are logged as block transactions. The approval process for new blocks of transactions is a collaborative process between the members. The operating mode of the blockchain defines the criteria for selecting members. The three operational modes in blockchain can be distinguished as public, private, and consortium operation modes.

Public blockchain enables any person or organization to instantiate a blockchain node and connect to the blockchain network. Depending on the conditions of the consensus protocol, any member in the network can contribute to the network by participating and verifying the transactions. Bitcoin [16] and Ethereum[124] are well-known examples of public blockchains. The public blockchain ledger is consistently stored in all members' nodes. Each member obtains an opportunity to mine a block, depending on the conditions. For example, in Bitcoin, the mining node must prove a certain amount of work to be elected for mining. In contrast, the private blockchain networks restrict access to the network. The contribution to the blockchain, including verifying and adding new transactions to the ledger, is restricted to a limited number of members. The participants of private blockchain networks are trusted entities. In industrial applications, a private blockchain is widely used as the members' collaborative members must be trusted. For example, in healthcare IIoT and data-sharing blockchain applications, the members must be limited to the healthcare domain partners as the medical data is a sensitive and access-controlled commodity. R3 Corda [125] and Hyperledger Fabric [104] are significant examples of private blockchain platforms. A consortium blockchain is an intermediate model between public and private blockchains. Consortium blockchains enable certain types of members to join the network for specific purposes. Regulatory governance is one of the most prominent examples that enable regulatory authorities to connect to the blockchain network even though the contribution to the network is limited. R3 corda [126] is also operable as a consortium blockchain.

2.8.5 Impact of slowly adaptive adversaries in blockchain

The resistance to slowly adaptive adversaries is an essential consideration in the design of reputation-based consensus protocols. Slowly adaptive adversaries first observe the system and then corrupt the publicly visible high-reputation mining nodes. This potentially threatens reputation-based consensus protocols [87, 127, 128, 88, 85]. The attack is considered in the state-of-art blockchain protocols [129, 130] with potential solutions [131]. However, it is important to consider efficiently securing the blockchain network from slowly adaptive adversaries for production-grade deployments.

2.8.6 Significance of fog computing for blockchain

IIoT allows the interconnection of billions or even trillions of objects via the Internet and is growing tremendously. IIoT represents a network of physical objects or devices integrated with manufacturing processes, consisting of sensors and actuators, enabling many applications and services by exchanging data with each other and the end user. This requires computing-intensive operations, huge storage needs, and real-time communication, which cloud service providers cannot always guarantee most efficiently. Therefore, fog computing has been introduced, in which fog devices perform the first data processing activities, significantly reducing the application delay. Therefore, fog computing is one of the most widely used computational service architectures in IIoT. Fog computing transfers the computational power from the cloud to the edge, which enables the computational resource-restricted IIoT to offload computational functions to the edge layer. Industrial processes require most tasks, such as real-time big data mining, concurrent data collection, data structuring, and filtering, to be performed closer to the IIoT deployment premises to eliminate delays and ensure security requirements [132]. In [133], a fog-based architecture has been proposed for a smart manufacturing environment addressing the latency issues of cloud-based architectures.

2.9 Applicability of the background concepts into the research

Section 2.1 introduces the IoT with three-layered architecture and different capabilities, limitations, and requirements to identify the significance of efficiency in this research. Section 2.2 emphasized the transformation of IIoT as a specialized IoT. The potential attacks of the IIoT have been discussed in the section, which was utilized in the problem definition of the research. Section 2.3 includes the definitions of the terms to avoid ambiguities in explaining the work. Section 2.4 explains network slicing and brokering, which is a key contribution to the research. Section 2.6 explains the technical foundations of the proposed research in the IIoT authentication and encryption domain. Section 2.5 emphasizes the requirement of reliable IoT data formulation. Finally, Section 2.8 explains the distinguishing capabilities of blockchain and the relevant concepts to develop security services in the IIoT.

The next chapter presents a technical review of the state of the art.

3 Technical review of the state of the art

This chapter includes a technical review of the state-of-the-art approaches to the research questions. Section 3.1 explains state-of-the-art IIoT authentication and IIoT-Fog-Cloud key establishment distinguished as centralized and decentralized approaches. Section 3.2 reviews the related works in network slice brokering from two perspectives as centralized and decentralized approaches. Section 3.3 reviews the state-of-the-art blockchain for IIoT data formulation.

3.1 IIoT authentication and IIoT-fog-cloud key establishment

IIoT node authentication and IIoT-Fog-Cloud key establishment are mandatory security requirements to ensure the security of fog and cloud-integrated manufacturing systems. The authentication of IIoT nodes ensures that only authorized devices in carry out data acquisition and control physical systems. Exchanging the messages between authenticated IIoT nodes and cloud services ensures the integrity of messages. Furthermore, IIoT-Fog-Cloud channel key establishment is important to ensure the confidentiality of IIoT-Cloud messages exchanged. Confidentiality is a fundamental requirement of IIoT security and is also important as IIoT communication requires message transit over untrusted channels, including the Internet. However, the efficiency in securing the IIoT is important to preserve the scalability and performance requirements anticipated in IIoT. This section recapitulates the key state-of-the-art research on IoT authentication and key establishment, which were distinguished as centralized and decentralized techniques.

3.1.1 Centralized techniques

PKI is one of the promising solutions to eliminate security risks. This ensures authentication and communication integrity by using public key certificates. IIoT communications are mostly performed in a wireless medium open to many attackers. The inclusion of sufficient security mechanisms should be guaranteed[90]. In particular, authentication of legitimate IoT devices is a very important feature[134]. Authentication is typically addressed through certificates issued by a particular CA. In particular, in IIoT, the Elliptic Curve Qu-Van Stone certificates offer a lightweight solution. However, as IoT devices are put in an open field, they can be more easily attacked and hijacked. Consequently, it should be possible to efficiently organize the revocation of certificates issued by multiple CAs. This is typically done by consulting a Certificate Revocation List (CRL), which requires a lot of storage memory, is time-consuming, and not easily manageable in case different CAs are involved In [135] and [136], the authors highlight the key information security challenges in the IIoT context and elaborate on the requirement for trust establishment. In addition, the IIoT system suffers from high latency due to cloud integration [137]. In [138], another fog-based authentication and key agreement protocol was proposed, which was limited to elliptic curve operations and does not require user interaction on IoT devices. Sciancalepore et al. [139] proposed an ECQV implicit certificate based key management protocol for mobile and IoT. However, the proposed architecture [139] relies on a Trusted Third Party(TTP) that could be a single point of failure. Furthermore, handling the sheer volume of requests for cryptographic operations in a centralized TTP is challenging in scaled-up environments.

3.1.2 Decentralized techniques

This research explores the significance of decentralized techniques that facilitate IoT security services without incorporating blockchain. Fremantle et al.[140] proposed a federated identity management protocol for IoT with MQTT and OAuth. In Cantor and Shibboleth architecture[141], federated identity management that provides multiple web applications was proposed. Dammak et al.[142] proposed a decentralized group key management protocol for dynamic access control of IoT. Abdmeziem et al. [143] proposed a decentralized and batch-based group key management protocol for mobile IoT. Kumar et al.[144] a novel decentralized group key management protocol for cloud-based vehicular IoT networks. Perrig et al.[145] proposed a security service platform that provides data confidentiality, integrity, and authentication. The common feature of each is that each decentralized technique relies on a trusted service that manages/generates the keys.

In contrast to the decentralized techniques reviewed above, blockchain has immense potential to improve IIoT security with enhanced trust with consensus. By leveraging distributed smart contracts, IIoT nodes can gain access to security services deployed on the edge layer faster when compared with the services hosted in the cloud. The immutable ledger ensures accountability and non-repudiation of the transactions committed. A comprehensive discussion on the role of blockchain in the 5G and IoT with opportunities and challenges covered in [146]. IoT devices should be able to reach the fog devices authentically using certificates published on the distributed ledger by their CA. The fog node can easily verify the certificates' validity by invoking a query from the ledger. The servers and fog nodes with blockchain instances monitor the traffic and determine potentially malicious devices (e.g., through intrusion detection mechanisms). If so, the server revokes the corresponding certificate of the device and publishes the revocation on the ledger. Bouachir et al. [147] highlight the applicability of blockchain and fog computing for enhancing the security and service values of IIoT applications. Gadekallu et al. [148] present a review on the different applications of blockchain-enabled Edge of Things (EoT) The significance of blockchain for the smart manufacturing and Industry 4.0 is presented in [149, 150, 151] The research also distinguishes the scheme by [152] in which the blockchain is used to create a fully distributed access control system for IoT. However, the proposed architecture in [152] suffers from scalability limitations concerning storage, and the author also reflected on the requirement of transaction fees for the public blockchain network as a deployment environment. The applications of blockchain for smart manufacturing-oriented IoT security is presented in [153, 154]. Shen et al. [155] propose a blockchain-assisted IoT device authentication scheme based on identity-based signature schemes. However, the authors noted the communication overhead as a significant limitation of the proposal. In addition, the storage overhead of public key certificates in the ledger is a potential limitation when the system requires scaling up. In [156], a symmetric key-based scheme for the fog architecture has been proposed, including mutual authentication, anonymity and unlinkability. Dorri et al. [157] proposed a scalable and blockchain-based security service for resource-restricted IoT networks. Kumar et al. [158] proposed a blockchain-based framework that delivers value additions to the IIoT networks, including IIoT security. Wang et al. [159] proposed a lightweight certificate-less authentication scheme for IIoT. Singla et al. [160] and Qin et al. [161] applied public blockchain to facilitate IIoT authentication. Yakubov et al. proposed [162] a hybrid architecture of blockchain and PKI to authenticate IoT.

3.2 Secured network slice brokering

Network slicing was introduced as a key technological element in the 5G and beyond networks to provide specialized network services for different use cases to support multi-tenant and multi-operator environments with advanced consumer demands. In IIoT networks, the network slice broker operates as a stand-alone third party that communicates with the network slice managers of the network operators. This section focuses on the key state-of-the-art network slice brokering architectures distinguished as centralised and decentralized techniques.

3.2.1 Centralized techniques

Boubendir et al. [163] proposed a federated operational architecture to share network resources such as connectivity, storage, and computational resources to the consuming stakeholders. However, the performance indicators in the experimental evaluation, such as the estimated slice onboarding time up to 3 minutes, reflect the proposed architecture's scalability limitations in real-time application scenarios. Sciancalepore et al. [164] proposed a low-complexity online network slice brokering solution that maximizes multiplexing gains and aligns with the 3GPP architecture. Pawani et al. [71] proposed a secured key exchange scheme with secure multi-party computation which is tolerant to DoS attacks by establishing direct communication in between slices instead of using third-party monitoring applications. Sattar and Matrawy[72] propose a twofold network isolation model using inter-slice and intra-slice isolation to mitigate DOS attacks. The proposed architecture utilizes a mathematical model to ensure security through slice isolation. Mamolar et al. [73] proposed edge computing-oriented DDoS attack mitigation system in the 5G multi-tenant infrastructure Moudoud et al. [74] propose a Markov stochastic process based security model to detect DoS attacks in the 5G IoT ecosystems. Lalropuia and Gupta [75] proposed a Bayesian-game-based model to identify the bandwidth spoofing DoS attacks and the best response strategy. Swami et al. [165] presented a comprehensive study on DDoS attacks in SDN contexts along with a classification of DDoS defense mechanisms.

3.2.2 Blockchain-based techniques

Backman et al. [166] highlighted the significance of blockchain as an additional trust layer for NSB. The authors highlighted the distinguishing capability of blockchain as a collaborative service that enables every tenant, actor, and stakeholder to participate in slice leasing activities. Valtanen et al. [167] present an analysis of a blockchain-based slice brokering use case as a resource configuration framework from the perspective of industrial automation. The authors highlight the distinguishing capabilities of blockchain to reduce the service creation time and the capability to enable manufacturing equipment to acquire the network slices efficiently and autonomously. However, the capability of smart contracts for automated SLA establishment was not utilized in the proposed architecture. Afraz et al. [168] defined network slice as a tradable commodity with parameters such as RAN, computational resources, and storage. The proposed architecture utilizes the consensus mechanism to collaboratively establish consensus in a double auctioning process. However, since the slice is traded as a single commodity, the potential options for the consumers will be limited as the candidate resource provider must have all the resource types to become a qualified candidate resource provider to deliver the consumer-requested slice. Serving the slice as a single commodity restricts the potential options to the consumers and will reduce the impact of competitiveness in the consumer's perspective. Zanzi et al. [169] proposed an NSBChain, which is a hierarchical blockchain architecture for network slice brokering. However, the slice selection algorithm only relies on the lowest price of the entire slice. In such scenarios, the resource providers with particular resources at cost-effective prices than those capable of providing entire resource providers will remain under-utilized. Such scenarios will discourage the resource providers to competitively participating in resource trading with the tenants. Nour et al. [170] proposed a blockchain-based network slice brokering mechanism with anonymous transactions. Antevski and Bernardos [171] proposed a distributed-ledger-based solution for the federation of 5G network services through smart contracts. Lin et al. [172] proposed a novel consensus protocol to enhance the accountability of slice brokering using blockchain.

3.3 Reliable IIoT data formulation with consensus

The data-driven innovations facilitate the future of industrial domains with more data-oriented capabilities. Reliable IoT data formulation is fundamental for intelligent decision-making, driving insights and maximizing data utilisation. However, due to the heterogeneous nature of IIoT, establishing reliability is challenging [24]. Theodouli et al.[173] presented a blockchain-based architecture for healthcare data sharing. However, the proposed architecture lacks the identification of malicious data formulation via the impersonation of patients. Ghadamyari et al.[174] facilitate on-chain computation on healthcare data using Paillier encryption. The impact on the statistical analysis incurred by malicious data was not evaluated by the authors in [174]. Shen et al. [175] proposed the MedBlock solution, which facilitates patient data storage and data sharing. However, the proposed architecture in [175] suffers from the existence of malicious patients who deliberately provide invalid data. Ito et al. [176] highlight the potential of blockchain for privacy-preserved personal health data sharing. Ekblaw et al. [177] propose MedRec, a PoW consensus-based medical information management platform. The proposed architecture in [177] utilizes PoW consensus protocol which is not energy efficient and sustainable in realistic scaled-up scenarios. Furthermore, the distributed nature of the public ledger sums up several limitations, including privacy [178], which makes the integration of blockchain challenging for healthcare applications [179]. These challenges include data privacy preservation in public ledger data, derivation of analytical insights from the ledger data, fair and efficient consensus that does not consume above-average computational resources, and performance features such as lower latency and higher throughput, and scalability. Huang et al. [180] propose a credit-based consensus protocol. In proof of familiarity presented in[105], members of the blockchain network who are the highest in terms of familiarity with a particular disease contribute to medical decision-making. Repchain [181] is an IoT reputation-based consensus mechanism. However, the reputation-based consensus is vulnerable to the slowly adaptive adversaries that monitor the network and corrupt the high-reputation blockchain nodes.

The next chapter reviews the state of art approaches to the research questions defined in the thesis.

4 Research contributions

This chapter elaborates on the contribution of the original publications in detail. Firstly, the proposed solutions for efficient IIoT authentication and IoT-Fog-Cloud key establishment. Section 4.1 emphasizes the problem formulation and the synthesizing of the research questions based on the literature review. Section 4.2 explains the research methodology in the research. Section 4.3 explains the components of each research question as threats and limitations. Section 4.4 outlines the individuals' contribution to the thesis. Section 4.5, Section 4.6, and Section 4.7 explain the contribution of the results to RQ1, RQ2, and RQ3, respectively. Finally, Section 4.8 explains the security analysis with the thesis's contribution.

4.1 Motivation and problem formulation

IIoT has revolutionized various sectors, including manufacturing, healthcare, and energy, integrating 5G and beyond networks. However, the security of the IIoT systems remains a core feature[45] to ensure secured functions of IIoT networks. Establishing trust in manufacturing/monitoring equipment through authentication is a vital security requirement to ensure product authenticity and manufacturing lifecycle consistency. In addition to the trust, ensuring privacy over the untrusted channels to secure sensitive intellectual information exchanged in the manufacturing lifecycle is important to ensure confidentiality. Scalability is an overall requirement to ensure that securing the IIoT systems does not compromise efficiency and does not incur storage as well as extensive computational overheads. However, centralized IoT authentication systems architecture cannot scale up the IIoT networks as the centralized security service is a bottleneck that limits the capabilities in a production-grade deployment setup. The blockchain-based IIoT authentication and key establishment systems suffer from storage scalability limitations as the blockchain continuously expands with the system's evolution[182, 183]. Purging/removing the ledger will violate the blockchain's fundamental immutability. Furthermore, the public ledger records of authentication-related information enable malicious/curious parties to obtain insights into the tenants that compromise privacy[178]. The existing literature predominantly focuses on the X509 certificate's lack of efficient storage and network bandwidth utilization[184]. The key exchanges over the network and storage in the databases impose extensive overhead when the network is scaled up. The literature that utilizes blockchain-based smart contracts to improve IIoT security lacks anonymity and unlinkability, as the ledger is shared between the blockchain network members. Identifying these research gaps, this research formulates the question RQ1 as follows.

- **RQ1: How do the blockchain-based smart contracts efficiently authenticate IoT and establish IoT-Fog-Cloud end-to-end encryption?**

MNOs and local 5G operators provide the infrastructure, including computational functions, base station operations, and network slice lifecycle management. Network slicing plays a crucial role in IIoT networks with ensured service differentiation and isolation for individualized tenant requirements. The reviewed literature reflects the potential use of network slice brokering mechanisms to facilitate the autonomous resource allocation of network slicing in 5G and beyond networks[167]. The impact of DoS/DDoS attacks disrupts the functions of network slice brokers in slice delivery to legitimate tenants [185]. Furthermore, trading a slice as a single commodity reduces the resource provider utilization, making the resource providers unable to fully contribute in slice brokering[169] Identifying these research gaps, this research formulates the question RQ2 as follows.

- **RQ2: How do blockchain-based smart contracts secure a network slice broker from DoS/DDoS attacks and facilitate efficient network slice brokering?**

The IIoT sensors connected to the manufacturing systems generate massive data from heterogeneous sources. The reliability of the data is challenging due to the decentralized nature of IIoT networks and the potential for malicious data formulation from compromised devices. The presence of unreliable and malicious data affects the accuracy of intelligent decision-making, analysis, and sharing in industrial applications. The existing systems lack a data formulation mechanism that assesses the accuracy and reliability of data and filters out the invalid data before utilizing enterprise applications[87, 186, 175]. Cloud-based schemes are restricted to a single service instance and suffer from scalability limitations with a high transaction volume bottleneck and a single failure point with more risks for DoS attacks [187, 87]. Blockchain-based smart contracts enable decentralized data validation and the reliability/trust-based reputation scoring distinguishes reliable/trusted nodes for reliable decision making. However, blockchain-based, reputation-oriented consensus mechanisms are not resistant to attacks launched by slowly adaptive adversaries that attack higher reputation mining nodes in the system [181, 105, 180, 176]. Huang et al. [131] proposed zkRep that utilizes the Zero-Knowledge Succinct Non-Interactive Argument of Knowledge(zkSNARK) method for reputation score proofs. However, zkSNARK requires a trusted setup that imposes an extensive energy overhead in scaled-up environment. Furthermore, the network

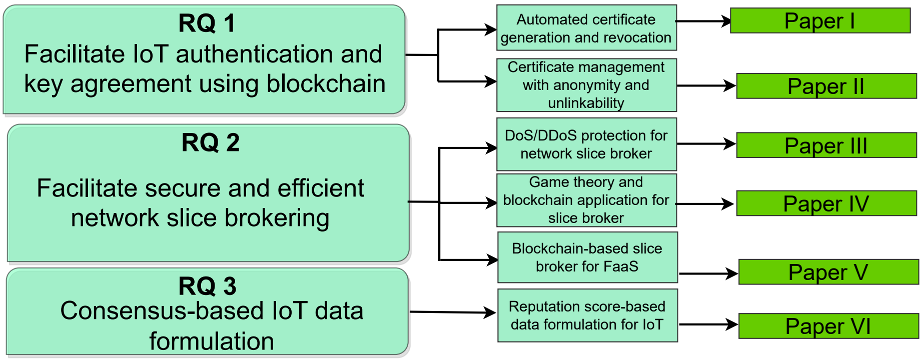
RQ 1
Facilitate IoT authentication and key agreement using blockchain
RQ 2
Facilitate secure and efficient network slice brokering
RQ 3
Consensus-based IoT data formulation
Automated certificate generation and revocation
Certificate management with anonymity and unlinkability
DoS/DDoS protection for network slice broker
Game theory and blockchain application for slice broker
Blockchain-based slice broker for FaaS
Reputation score-based data formulation for IoT
Paper I
Paper II
Paper III
Paper IV
Paper V
Paper VI

Fig. 5. Research questions.

overhead is quite higher in zkSNARK-based reputation score proofs. Identifying the limitations of the state of art, this research formulates the question RQ3 as follows.

- **RQ3: How do the reputation-score-based consensus mechanism can be efficiently utilized for secured and reliable IoT data formulation?**

Figure 5 reflects the research questions and the corresponding research articles.

4.2 Research methodology

The research identified the security requirement in IIoT systems, threats, and potential security services as illustrated in Subsection 2.2.3. The research investigated the potential of blockchain-based smart contracts to incorporate the identified security services to gain efficiency beyond the state-of-the-art with proven results from the experimental evaluations.

The research was mainly planned in three stages. The first stage was a preliminary study and literature review to examine the state-of-the-art work on the fundamentals of IoT/IIoT and how authentication is distinguished as centralized and decentralized techniques, and the novel efficient authentication and key establishment protocol addressing the limitations of state-of-the-art was developed using blockchain-based smart contracts. The primary outcomes of the proposed novel protocol include device authentication and IIoT-Fog-Cloud end-to-end key establishment with improved anonymity, unlinkability, storage efficiency, and reduced latency compared with the state-of-the-art.

The second stage investigates the potential attacks on 5G network slice brokers and the potential of blockchain-based techniques to defend the network slice broker against such attacks. Furthermore, the second stage investigates the potential of the Stackelberg game model to formulate efficient federated network slice creation for multi-operator and multi-tenant scenarios. The outcomes of stage two include a DoS/DDoS attack-resistant network slice broker with the incorporation of a Stackelberg game-based slice selection algorithm implemented as smart contracts.

Stage three investigates the applicability of reputation score to distinguish non-malicious IoT data. Furthermore, the consensus protocol utilizes BulletProof ZKP to achieve energy efficiency in the reputation score verification compared to the state-of-the-art. The consensus protocol utilizes the privacy-preserved reputation score verification to defend the blockchain network from the slowly adaptive adversaries that observe the high reputation IoT data formulating nodes and attacks.

All the authentication and key establishment protocols proposed in this thesis were validated in terms of their performance by numerical programmatic simulations and near-realistic implementations (Paper I and II). The proposed solutions were validated for performance and distinguished with the state of the art with partial implementations of the state of the art. Furthermore, in Paper III, the attacks were programmatically generated, and the proposed functions were implemented on the Hyperledger Fabric blockchain platform to evaluate the impact of the attacks on the NSB when the NSB was hardened with the proposed security mechanisms. Furthermore, in Paper IV and Paper V, the proposed algorithms were implemented using the Hyperledger Fabric blockchain platform to function as the slice broker integrated with the Katana slice manager and DevStack as the resource provider In Paper VI, the adaptive adversarial attacks were simulated using software programs. Furthermore, the energy consumption of the ZKP was evaluated using the Intel Power Gadget tool. In Paper VI, the proposed consensus protocol was modelled using PAT model checker[188] to evaluate the correctness. Raspberry Pi devices, cloud servers, and virtual machines on the laptops were used to appropriately simulate IIoT nodes, edge, and cloud infrastructure. The experimental evaluations include implementations of the state of the art and comparisons with the proposed works in different scenarios to distinguish the advancements in the proposed work.

4.3 Problem definition - threat modelling and efficiency limitations identification

Industrial IoT networks comprise heterogeneous specialized industry-oriented IoT devices such as sensors, actuators, manufacturing machines, etc. In state-of-art IoT networks[189], the IoT devices are connected to the edge computing nodes[4], cloud computing nodes[190] with 5G and beyond network connectivity[57].

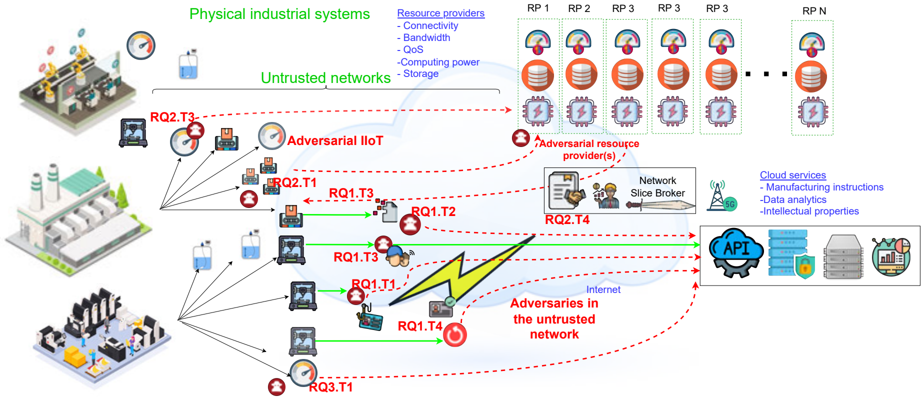

Fig. 6. Problem definition in IIoT systems.

This research formulates the threats with consideration of Dolev-Yao[191] attack model which applies to communication over untrusted networks such as the Internet as proposed in this thesis. In addition, this research incorporates edge and fog computing architecture that facilitates intermediary processing between IoT and cloud to yield efficiency in terms of latency.

Figure 6 reflects the architecture of IIoT network in 5G and points to the potential attacks.

1. **Identity impersonation attacks in manufacturing/monitoring IIoT (RQ1.T1):** The IIoT systems comprise heterogeneous sensors and actuators that have been connected over untrusted networks [190]. In the identity impersonation attacks of IIoT, an adversary that is connected to the untrusted network pretends to be a non-malicious IIoT node in the network and intentionally forges the manufacturing instructions/monitoring data that affects the product's authenticity and overall manufacturing lifecycle consistency. Furthermore, without mutual authentication, the untrusted IoT nodes, untrusted fog/edge devices and untrusted cloud expose the manufacturing systems to a massive risk of interfering with the manufacturing workflow consistency. Such circumstances degrade the trust of the entire manufacturing system. The research identifies several related works [160, 161, 162, 192] that propose PKI and digital certificates with blockchain integration[162] as solutions to eliminate identity impersonation attacks considered in the research. However, the research signified several limitations of the state of the art in scaled-up IoT networks that have evolved towards production-grade scale. More specifically, the PKI-based techniques [162] that utilize the X509 digital certificate[160] and blockchain-based

approach[192] for IoT authentication incur extensive overhead to the IIoT system in terms of certificate storage and network overhead as the networks require scalability. Incorporation of public blockchain[161] for the PKI integration is resource intensive with a non-tolerable latency with extensive storage overhead that emerges practical challenges in the adaptation towards resource-restricted IIoT networks.

2. **Manipulations/corruptions of IoT-Fog-Cloud manufacturing instructions/sensor data transferred over the untrusted networks(RQ1.T2):** The IIoT systems comprise of IoT-Cloud connectivity over untrusted networks [190]. The sensing data of the manufacturing process and manufacturing instructions, including 3D printing data[193] are generated from the intellectual property repositories in the cloud. The modified or corrupted manufacturing instructions will eradicate the product consistency, while the modified or corrupted sensor data will affect the monitoring service accuracy. Corrupted machine instructions or sensor data compromises the overall reliability and trust of the manufacturing system, with a significant potential to result in financial losses to enterprises. Ultimately, the end-to-end message manipulations eliminate one of the fundamental properties of security[194]: Confidentiality, Integrity and Availability, which is well-known as the CIA triad. The research identifies the impact of adversaries in the untrusted network that compromise the integrity of messages by modifying/corrupting them.
3. **Eavesdropping the sensitive manufacturing instructions/sensor data in IoT-Fog-Cloud channel over the untrusted network(RQ1.T3)** : The IIoT systems connect the IoT nodes, such as actuators and sensors, to transfer cloud-originated instructions of the manufacturing process as well as monitoring the manufacturing processes through sensors. Suppose the data transfer includes a transit over an untrusted network[190]. In that case, the adversaries can eavesdrop on sensitive information[195, 196], such as manufacturing instructions and sensor data, that compromise the privacy of the intellectual manufacturing instructions and manufacturing sensor data. It is challenging to rely on a single instance of trust service that manages the group keys [142, 143]. This research identifies the adversarial impacts as a significant threat that compromises the confidentiality of the fundamental properties of security[194]: Confidentiality, Integrity and Availability, which is well-known as CIA triad.
4. **Replay of IIoT authentication credentials to gain access(RQ1.T4):** Authentication of the IIoT nodes and cloud nodes is proposed in this research to establish trust and eliminate threats:RQ1.T1, RQ1.T2 and RQ1.T3. However, this research identifies the impact of the adversary in the untrusted network of the IoT-Cloud integrated system that replays authentication credentials[197]. In such scenarios, the adversary

eavesdrops on the authentication credentials of the legitimate node(s) and repeatedly sends legitimate authentication data to gain unauthorized access to the manufacturing systems to pretend as a non-malicious IIoT node.

5. **Threat prioritization and classification challenges in heterogeneous IIoT networks (RQ1.T5)** The consistent security service of IIoT networks must account for the adversarial presence in the IIoT nodes deployed in the system itself. The IIoT network comprises of heterogeneous IIoT nodes with diversified roles in the system. For efficient threat management and effective incident response, it is important to prioritize the threats [198] based on different criteria, such as the value of data assets formulated from the IoT[199] and corresponding security risks[200]. IDS is one of the most promising tools to detect intrusions in the IoT networks[201]. However, the prominent limitations of IDS, such as false positives[201] and false negatives[202] make the incident response actions challenging in IIoT networks with diversified application scenarios. More specifically, revocation of the issued certificate [203] for a false alarm incurs extensive overhead in terms of energy and network resources to [204]. Threat scoring[205] provides a numerical assessment on the risk, which is insightful on the incident response process. However, in IIoT networks, threat scoring as a centralized instance of service creates a bottleneck, and the incident response delay provides time window for the adversary to launch the attack even though the attack has already been detected by the IDS. Therefore, centralized threat-scoring schemes have obvious limitations.
6. **Transaction linkability on the consortium ledger(RQ1.T6):** The blockchain provides decentralized trust and transparency in digital certificate management[160, 161, 162, 192, 162] in IoT networks. However, the transparency feature of state-of-the-art blockchain-based proposals reflects business-confidential information on the ledger, which has been consistently shared among the consortium members. For example, if the blockchain-based certificate management system operates as a consortium-based decentralized service of multiple manufacturing entities, the ledger will be available among the members. In such cases, the honest and curious adversary has grounds to formulate insights on the scale of the manufacturing systems and the competitors' different varieties of manufacturing equipment by linking the available records.
7. **Extensive latency and storage overhead for managing in scaled-up IIoT networks(RQ1.L1)** The IIoT networks are required to support the scalability. The centralized PKI systems[206] for the IIoT creates a performance bottleneck when the number of IIoT nodes is scaled up. Moreover, the state of art blockchain-based [160, 161, 162, 192, 162] techniques suffer from the overhead of ever-growing

distributed ledger overhead. Thus, it is challenging to integrate in production-grade IIoT networks.

8. **Malicious resource requests sent by colluding IoT tenants(RQ2.T1)** :The industry-grade deployments of IIoT consist of a diversified tenant group. The research identifies the risk of DDoS attacks that can be launched by a malicious group of IoT tenants under an attacker's control and operate unlawfully towards a common ill objective. Every member of the colluding group of IIoT tenants sends a permissible number of requests to the NSB with the intention make the NSB and the resource providers are unavailable to the legitimate tenants. However, collectively, they might succeed in bringing down the services of the NSB and resource providers, which can result in overloading API-related message streams, memory overflows and the over-utilization of computational resources. Early detection of such a colluding group of IIoT tenants is relatively difficult compared to the malicious requests sent by a single tenant. To defend the IIoT network resource providers and NSB from such attacks, it is important to immediately detect and respond by restricting the NSB access to the adversarial tenants.
9. **Malicious resource requests sent by compromised individual IIoT tenants(RQ2.T2):** Compromised IIoT tenants can send extremely large numbers of resource requests (also called slice requests) with malicious intentions to an NSB (i.e., DoS attack). This leads to the generation of subsequent events within the brokering entity as per the sequential workflow of the NSB. For instance, a malicious request may consist of a large number of resource parameters that require resource-intensive execution In such a scenario, the relevant NSB's modules for each step will run extensively to perform different activities, including the creation of the slice blueprints and disseminating them to the MNOs. The high volume of transactions takes up computational resources and depletes the storage with malicious traffic. Thus, the NSB will be overloaded, quickly rendering the slicing service unavailable. Furthermore, the effects of the attacks will be reflected on the MNOs since the MNOs will continuously respond to the requests received from NSB under attack. The overall effect is that such malicious requests will overshadow the legitimate resource requests in the NSB.
10. **Malicious resource offers sent by colluding MNOs(RQ2.T3):** A subset of MNOs under external malicious control can be made to collude and send bogus resource offers to NSBs (i.e., DDoS attack). This kind of attack can trap the slice selection algorithm and hog the resources. Thereby, the non-malicious tenants and resource providers will hinder the slice brokering process. The tenants will be failed with the service delivery as required.

11. **Malicious resource offers sent by compromised MNOs(RQ2.T4):** An NSB can be potentially affected by malicious resource offers sent by MNOs (i.e., a DoS attack). The severity depends on the computationally intensive nature of the selection algorithm powering the NSB. Moreover, malicious resource offers sent by a compromised MNO may intentionally include numerical values, resulting in an overflow of the memory heap of the NSB, thereby impacting its capabilities. Furthermore, the malicious MNOs may intentionally send messages of an extensive length, which overloads the messaging protocols and data buffers of the API services of the NSB. Thus, the NSB may fail to receive the legitimate resource offers under such an attack.
12. **Extensive financial costs to the consumers and under-utilization of resource providers of network slice(RQ2.L1),** : The sixth-generation (6G) telecommunication infrastructure is expected to facilitate more diversified consumer requirements arising from various emerging use cases with on-demand creation of multiple End-to-End (E2E) logical networks over a common physical (mobile network) infrastructure. Factory-as-a-Service (FaaS) allows the agility of adaptation of the manufacturing process by identifying the supply chain and user requirements in IIoT. To enable FaaS with the help of networking and cloud services, it is always essential to have non-interrupting IT and telecommunication services[207], [208, 209]. When an IIoT site forms as FaaS, it should scale up or down operations against the new engagements with higher flexibility. Instead of buying a slice from a single service provider, the operations in FaaS will have higher flexibility to acquire them from an open marketplace with access to multiple resource providers (RPs) in real-time. Many research efforts have already been taken to investigate how to combine blockchain and 5G network slicing technology [210] to leverage decentralization and data provenance. However, only a few works are explicitly focusing on developing an NS brokering framework using blockchain [163] and they are still not close enough to the actual deployment phase in a multi-operator multi-tenant platform, which is foreseen in the next-generation networks. In [166], blockchain is introduced as an additional trust layer in slice broker for trading and dynamic billing. The blockchain-based slice brokering mechanism in [167] uses smart contracts to enable dynamic and autonomous slice management.

    Moreover, the state of the arts does not provide any cognitive slice selection mechanisms to formulate federated network slices based on resource demand and availability. Therefore, the number of resource providers is limited to cater for the dynamic requirements of the multi-operator and multi-tenant scenarios, making the emergers less competitive.

13. **Repudiation and disputes in Secured Service Level Agreement establishment(RQ2.T5):** The network slice broker must invoke the security services and meet the security levels requested by the consumers. Integrating the predefined security service level agreements (SSLAs) [211] with the corresponding resource providers is necessary. SSLA is the primary instrument that documents the use case of the network slice, performance standards, lifetime, and roles and responsibilities[212] of each resource provider of the network slice and the consumer of the network slice. More specifically, the QoS and security requirements, such as encryption key sizes in different security services, will be included in the SSLA[213]. The real-time SSLA establishment is required for a multi-provider, multi-tenant environment. Non-repudiation[214] in SSLA is one of the most prominent requirements that must be preserved for the consistency of security. However, SSLA establishment requires dynamic and advanced automation with real-time functions while preserving the non-repudiation properties in multi-operator and multi-tenant scenarios. The resource providers and tenants are the two types of parties that establish contractual agreements on the network slice. If the resource providers violate the SSLA by failing to deliver the appropriate service level(Eg. QoS, security etc.), the SSLA provides evidence to proceed with dispute resolution action.
14. **False data injection to the IIoT formulated data(RQ3.T1)**: IIoT can be classified into two main forms based on applications and use cases as sensors and actuators[214]. Sensors measure physical phenomena and generate data that corresponds with the physical events. Actuators perform physical actions based on the functional commands received from IoT-controlling services. Sensor-formulated data is the preliminary material for effective analysis and decision-making. However, due to the heterogeneous nature of IoT deployment models in 5G and beyond networks, the establishment of the reliability on data is challenging [24] with a wider potential risk for malicious data manipulations. When the adversarial IIoT sensors deliberately inject malicious data/modify the correct data, the applications that derive insights from the data drive the IIoT analytical applications towards incorrect insights. Implementing a data validation to identify the malicious data as a centralized service in a production-grade IIoT environment is not a trustworthy approach from the security perspective as an adversarial validation service can deliberately falsify the data. IoT sensor data validation frameworks[80, 81, 82, 83] provide conditions to distinguish the compliant and non-compliant data based on several pre-defined guidelines. However, implementing a data validation as a centralized service in a production-grade IIoT environment is a significant challenge that creates a bottleneck

with a massive communication overhead to pass-through the all IIoT data in a centralized data validation service.

15. **Slowly adaptive adversarial impact(RQ3.T2)**: The resistance to slowly adaptive adversaries is an essential consideration in the design of reputation-based consensus protocols. The slowly adaptive adversaries first observe the system and corrupt the publicly visible high-reputation mining nodes is a potential threat to the reputation-based consensus protocols [87, 127, 128, 88, 85]. The attack is studied in the state-of-art blockchain protocols [129, 130]. Huang et al. proposed a potential solution[131] for a slowly adaptive attack, and the key limitation is the requirement of a trusted party to manage the cryptographic keys of the proof. The attackers identify the highest reputation score mining nodes and attack them up to the budget. This will eventually make them unavailable for mining. When the top mining nodes are unavailable for mining, the mining nodes with a lower reputation score (than the group of victimized nodes) will be elected for mining.
16. **Extensive energy and bandwidth overhead to defend the network from adaptive adversaries (RQ3.L2)**: Securing the reputation score with provable encryption is one of the possible techniques to defend the high-reputation nodes. However, the key generation for reputation score proof that relies on the trusted parties [131] incurs extensive energy overhead to generate the cryptographic keys, limiting the scalability from the energy consumption perspective.
17. **Extensive latency and challenges in establishment of the trust on centralized encryption services(RQ3.T3)**: Encrypting data with the provisions to derive important insights on the encrypted data is a widely used approach in IIoT, anticipating improved privacy. For example, state-of-art medical diagnosis frameworks such as [87] enable encryption of medical records and usage for real-time medical diagnosis without compromising the individual privacy of medical records. However, in addition to the performance limitations such as latency challenges of the centralized architecture of the cloud-based services, cloud-based services are prone to the targetted attacks[215] and DoS attacks[15]. Furthermore, the centralized databases converge the trust towards a single point, which is prone to database targetted attacks[216].
18. **Fairness limitations in the reputation-based consensus protocols(RQ3.L3)**: Fairness is a crucial feature of a blockchain network. In principle, a blockchain is a decentralized network. Thus, all nodes must have a similar right to mine a block within the evolution of the blockchain lifecycle. The research experimented with evaluating two critical indicators of fairness in these experiments. Furthermore, to compare the advantage of mining node utilization with a state-of-art reputation

index-based consensus mechanism, the research partially implemented PoF [105] in our environment and performed the same experiment.

4.4 Contribution of the thesis

The thesis contributes from three different perspectives to establish decentralized and efficient security services in IIoT networks.

Paper I and Paper II address the first research question, which focuses on efficient and decentralized IIoT authentication and IIoT-Fog-Cloud confidentiality. In Paper I, ECQV certificate-based key establishment protocol is proposed for IoT with automated revocation using smart contracts. The author has proposed the reputation-based certificate revocation scheme. The author was responsible for designing the key establishment protocol, implemented in the Hyperledger Fabric blockchain platform, evaluating a deployment on Raspberry Pi devices, and analyzing the protocol with storage scalability and improved latency. Paper II was an extension of the proposed protocol in Paper I, with improved anonymity and unlinkability using the Schnorr algorithm-based Non-Interactive Zero Knowledge Proof(NIZKP) on the blockchain. The author and Prof. An Braeken proposed the idea of exploiting the implicit certificates on blockchain and NIZKP to ensure anonymity and unlinkability. Dr. Madhusanka Liyanage and Prof. Ylianttila supervised the entire work with active contributions on reviews to improve the paper. Paper II utilizes smart contracts to automatically generate ECQV certificates for IoT node authentication and propose to integrate scalable decentralized storage to improve the storage scalability. The protocol was designed during the candidate's research visit to Vrije Universitet Brussel with the support of Prof. An Braeken. Dr. Madhusanka Liyanage provided a significant contribution on the implementation and evaluation of the proposed work. Prof. Ylianttila was the supervisor.

The second research contribution includes designing and evaluating of the efficient and secured network slice brokering for 5G and beyond networks. Paper III investigates the impact of the DoS/DDoS attacks on the network slice broker and the potential of blockchain-based smart contracts to mitigate the attack. Paper III proposes a profiling mechanism to the tenants and resource providers to define the maximum bounds of resource utilization requests from the available resource providers. The smart contracts are encoded with the profiling rules and security service blockchain validates each request before sending to the network slice broker. The security service blockchain filters out malicious resource requests to defend the network slice broker. For Paper III, the candidate came up with the idea and contributed to the implementation and analysis of the profiling framework. Dr. Anshuman Kalla, Dr. Pawani Porambage, and

Dr. Madhusanka Liyanage provided critical comments on the design and evaluation of the proposed architecture. Prof. Ylianttila was the supervisor.

Paper IV investigates the potential of blockchain to efficiently facilitate network slice brokering mechanisms in multi-operator and multi-tenant scenarios. The initial idea of applying the Stackelberg Game model to the network slice brokering was from Dr. Pawani Porambage. The candidate has modelled the network slice brokering scenario into the Stackelberg Game model by distinguishing the resource providers and tenants as the two players. The Stackelberg game model is utilized to find the best matching network slice from the available resources through federation, with maximized profits to the resource providers and lower prices to the tenants. Dr. Anshuman and Dr. Madhusanka has provided insights on the implementation and evaluation. Prof. Ylianttila was the supervisor.

Paper V is an extension of the initial concept of Paper IV to apply the Stackelberg game model in the facilitation of factory as a service. Paper V proposes facilitating the automated establishment of service-level agreements using smart contracts. The objective of the Stackelberg game is to find the Nash equilibrium where no player intends to deviate from its strategy after considering its' opponent's choice. The network slice broker operates as a mediator in the slice brokering process. The candidate has extended the Stackelberg game model-based proposal to the factory-as-a-service facilitation. Nisita Weerasinghe has contributed on the Secured Service Level Agreement(SSLA) integration for the experiment evaluation. Dr. Madhusanka Liyanage has provided inputs to the experimental evaluation. Prof. Ylianttila was the supervisor.

Paper VI emphasizes the potential of consensus protocol for IoT data formulation based on the reputation score of the IoT nodes that generate IoT data. Furthermore, the BulletProof ZKP was utilized to identify the high-reputation IoT nodes without proving the reputation score, as a preventive measure to defend against slowly adaptive adversaries' attacks. The initial idea of a reputation score was proposed by the candidate. Dr. Pawani and Dr. Madhusanka provided inputs on the implementation and evaluation Prof. Ylianttila was the supervisor.

4.5 Efficient IIoT authentication and key establishment

4.5.1 Decentralized service architecture for efficient IIoT authentication and key establishment

Figure 7 reflects the architecture of a fog-enabled IIoT system. The first research question of this thesis addresses the design of efficient authentication and key establishment service architecture for IIoT that preserves anonymity and unlinkability. The security features of this research question include IoT node authentication and IoT-Fog-Cloud key establishment. The potential attacks considered in this research question include device spoofing attacks, MiTM attacks, and replay attacks of key establishment-related messages. The efficiency features of this research question include the lower latency on certificate generation, certificate access, storage scalability, and bandwidth utilization efficiency in authenticating IIoT nodes. Paper I proposes a novel decentralized service architecture for automated certificate lifecycle management in IoT. In Paper I, ECQV certificates are used to authenticate the IoT nodes. The ECQV certificates yield a storage consumption advantage compared to X509 certificates due to the shorter bit length of the public key and certificate[184]. Furthermore, the decentralized certificate management architecture is integrated with IDS to receive updates on malicious events of the authenticated IoT nodes. The smart contract defines the rules to automatically evaluate the threat score based on the malicious events identified by the IDS. The smart contract defines the threshold value of a threat score to automatically revoke the ECQV certificate. The proposed architecture eliminates the single instance CRL of the CA by the distributed ledger.

The computing infrastructure for the experiments consisted of Raspberry Pi 3 Model B V1.2 devices connected to the wireless local area network (WLAN) with a 5G internet connectivity. The Raspberry Pi devices operated as fog nodes and the virtual machine as the blockchain service running on the edge computing node The Raspberry Pi devices connected to the WLAN and the blockchain service were operated on a virtual machine connected by bridging through the wireless adapter of the host machine. The role of the virtual machine was expected to be identical to the edge computing node running in the network. The blockchain service was implemented using the Hyperledger Fabric blockchain network. The smart contract for the certificate revocation was implemented using Java programming language. The BouncyCastle cryptographic library was used to implement the associated cryptographic key generation.

Paper II extends the decentralized ECQV lifecycle management system with improved scalability, ensuring anonymity and unlinkability. As proposed in Paper I, the distributed ledger formulates cryptographically integrity-preserved records of the ECQV certificates corresponding to the IoT nodes. Paper II proposes to integrate an off-chain distributed extended storage service that preserves data integrity as an extension of the distributed ledger. The anonymity and unlinkability were preserved using the hashing techniques and non-interactive ZKP in the blockchain transaction records. Furthermore, the extended ledger storage improves the storage scalability of the proposed architecture beyond the state of the art. The proposed protocol facilitates automated dynamic

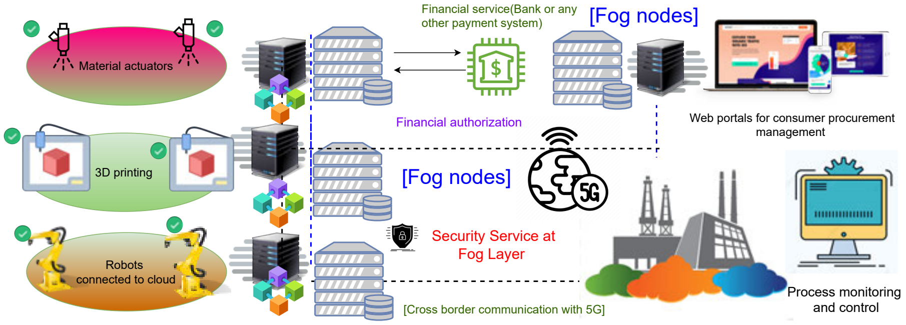
Financial service(Bank or any other payment system)
[Fog nodes]
Material actuators
Financial authorization
Web portals for consumer procurement management
3D printing
[Fog nodes]
5G
Security Service at Fog Layer
Robots connected to cloud
Process monitoring and control
[Cross border communication with 5G]

Fig. 7. Overview of the proposed architecture (Reprinted, with permission, from Paper II © 2022 IEEE).

ECQV certificate generation per a pre-defined number of IoT-Fog-Cloud messages. It establishes a dynamic session key to encrypt the exchanged messages between IoT-Fog-Cloud channels in the manufacturing operations. The dynamic exchange of authentication and encryption keys minimizes the impact of key compromise as the lifetime of authentication and session encryption keys is limited to the next session's ECQV certificate generation and session key establishment. The proposed key exchange mechanism resists replay attacks as a sequence number identifies each message.

The proposed authentication and key establishment protocol in Paper II consists of two phases. In Phase, I, the applicable IoT node for the manufacturing function(eg. 3D printers, actuators) registers on the system. Once the registration is completed, the identity information of the IoT node is stored at the extended storage and the storage pointer corresponding to the ECQV certificate is stored in the ledger. At registration, the number of dynamic certificate generation and the number of transactions per a dynamic certificate are registered.

Paper II proposed protocol was implemented and evaluated to distinguish the latency advantage of cloud-based PKI solutions for IoT node certificate access, storage utilization advantage, and scalability. The system was implemented using the Hyperledger Fabric blockchain platform as the blockchain platform and Inter Planetary File System (IPFS) as the distributed storage system to extend the storage. The results yielded reduced latency in certificate access preceded for credential verification of IoT nodes in certificate verification scenario compared with the state of art[217]. The proposed lightweight ECQV certificates and integration of off-chain storage yield a lower blockchain storage utilization overhead in a scaled-up environment when compared with state of the art blockchain-based IoT authentication systems [182, 183]. Finally, the authentication key size in the proposal reduces the network overhead in authentication scenarios that exchange the public keys over the network when compared with the state of art[155] for a similar security level. Overall, the proposed decentralized service architecture yields request processing efficiency through lower latency, blockchain storage utilization efficiency through lower key sizes with storage service integration, and network bandwidth usage efficiency through lower key sizes needed for IoT authentication. Overall, the proposed decentralized service architecture provides IoT authentication and dynamic IoT-Fog-Cloud key establishment while preserving anonymity, unlinkability and efficiency, compared with the state of the art. Table 3, Table 4, and Table 5 shows selected numerical results to illustrate the advancement of the proposed architecture beyond the state of the art.

4.6 Decentralized and secured 5G network slice brokering

4.6.1 Decentralized service architecture for DoS/DDoS attack prevention in network slice bokering

The second research question investigated efficiently securing a network slice brokering mechanism using decentralized technologies. The research identified the impact of DoS/DDoS attacks on the network slice broker. Paper III proposed a novel security service blockchain (SSB) to protect the slice broker from DoS attacks by malicious tenants and MNOs. The main objective of the SSB is to ensure the persistent operation of the NSB for genuine members, even under the presence of compromised tenants and/or MNOs. In the proposed solution, the research utilizes SSB as a smart contract-based security gateway to validate each request and control the access of IoT tenants as well as MNOs to the slice broker. The proposed SSB ensures that all resource requests and resource offers committed to the slice broker are valid and approved by the consensus process of the dedicated secure blockchain network. Figure 8 shows the deployment of the proposed SSB mechanism.

The malicious resource requests which can be launched from compromised tenants and MNOs are explained in Section 2.4.3. The tenants and MNOs need to agree on the limits for the parameters as defined, prior to consuming the slice brokering service. Upon the consensus process, these profiles will be stored in the immutable ledger in the blockchain. The research proposes utilizing blockchain-based transaction profiles to verify each request the tenant and MNO launched to the SSB. After the transaction profile verification, if the requests are within the specified conditions, the SSB smart contract invokes NSB as an off-chain request to submit a legitimate request to the NSB.

The proposed architecture was implemented and evaluated on the Hyperledger Fabric blockchain platform. The evaluation simulated the resource providers' infrastructure

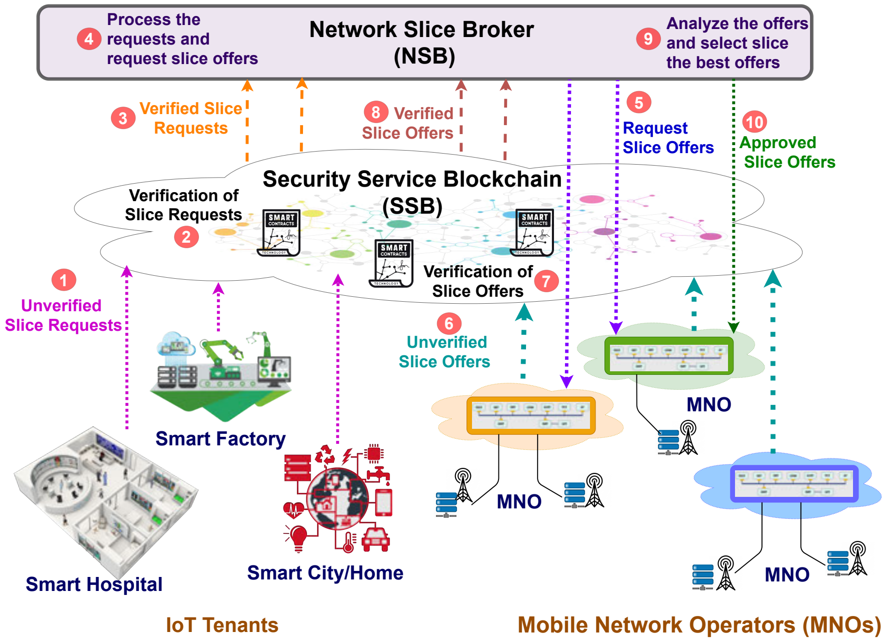
4 Process the requests and request slice offers
Network Slice Broker (NSB)
9 Analyze the offers and select slice the best offers
3 Verified Slice Requests
8 Verified Slice Offers
5 Request Slice Offers
10 Approved Slice Offers
Security Service Blockchain (SSB)
Verification of Slice Requests 2
SMART CONTRACTS
Verification of Slice Offers 7
1 Unverified Slice Requests
6 Unverified Slice Offers
Smart Factory
Smart Hospital
Smart City/Home
MNO
MNO
MNO
IoT Tenants
Mobile Network Operators (MNOs)

Fig. 8. Proposed Security Service Blockchain (Reprinted, with permission, from Paper III © 2021 IEEE).

using virtual machines and docker containers. The experimental results indicated a minimal impact to the legitimate tenants when attacks from malicious tenants and resource providers were present. The results reflect the latency increased than the proposed work for slice request processing of the legitimate tenants when the adversaries attack to the NSBs in art[185, 169]. The lower slice request processing latency for the legitimate requests of the proposed work in attack scenarios indicates the robustness of the proposed architecture to defend the slice broker. Selected numerical results from the state-of-the-art comparisons are shown in Table 3, Table 4, and Table 5.

4.6.2 Game theory-based decentralized, secured and efficient network slice brokering for IIoT

The second research question examines efficiently securing the network slice brokering mechanism using decentralized technologies. Papers IV and V elaborate on the applicability of blockchain and game theory to improve the security of network slice brokering for IoT. More specifically, the security services in the proposal include non-repudiation of service level agreements, ensured trust by smart contracts and resistance to DoS/DDoS attacks. The efficiency features include more resource provider utilization, reduced slice cost to the consumers, and lower latency in slice selection using smart contracts. Paper IV presented the concept of a secured and federated slice broker(SFSBroker) that incorporated blockchain for network slice brokering. The SFSBroker approach proposes a game-theoretic model to select the best match of tenants on one side and the MNOS or RPs on the other side as two player. This would ensure both the customer and service provider can reach their optimal utilities. RPs include virtualized resources, physical resources, and infrastructure for communication and computation. These resources are granted to the consumers as network slices where RAN, core network, computational infrastructure, and storage are potential candidates to be shared with the consumers as per requirement.

The SFSBroker acts as a global mediator between two ends to facilitate the delivery of network slices to the tenants acquired from infrastructure providers. The brokering mechanism should have a holistic knowledge of the consumers' and service providers' demand and supply status to provide a coherent and real-time service. The SFSbroker handles tasks such as receiving a slice request from tenants and disseminating it to RPs, selecting an optimal slice offer from a pool of proposals from the RPs, monitoring traffic and coordinating with orchestration services. This mechanism should cater to extensive service requests generated by the massive number of tenants with assured security (i.e., assure authentication, availability, privacy, trust, and access control).

The evaluation of the SFSBroker in this study included a Hyperledger Fabric-based implementation and Matlab-based simulation. The Hyperledger Fabric-based implementation was evaluated for scalability in scaled-up tenants and resource types. Furthermore, a partial implementation of NSBChain[169] was evaluated for the comparison of mean RP profit for a scaled-up number of parameters in a network slice.

Paper V elaborates on the blockchain and Game Theory-based network slice brokering with a use case scenario where a blockchain-based network slice broker enables Factory-as-a-Service. A blockchain-based NSB is a distributed trading platform to cater to federated network slices as required by each production site (Figure 9).

In this solution, the NSB is a distributed service that collects resource requests and security service requirements from each production site and designs the network slice based on the resource availability and ability to provide security services at the resource providers. For that, the NSB needs to keep records of resource availability and security services provided by each resource provider. An NSB blockchain service should run on each miner at the production and resource provider sites. Potential resource providers proposed in the secured NSB include MNOs, local 5G operators, and cloud

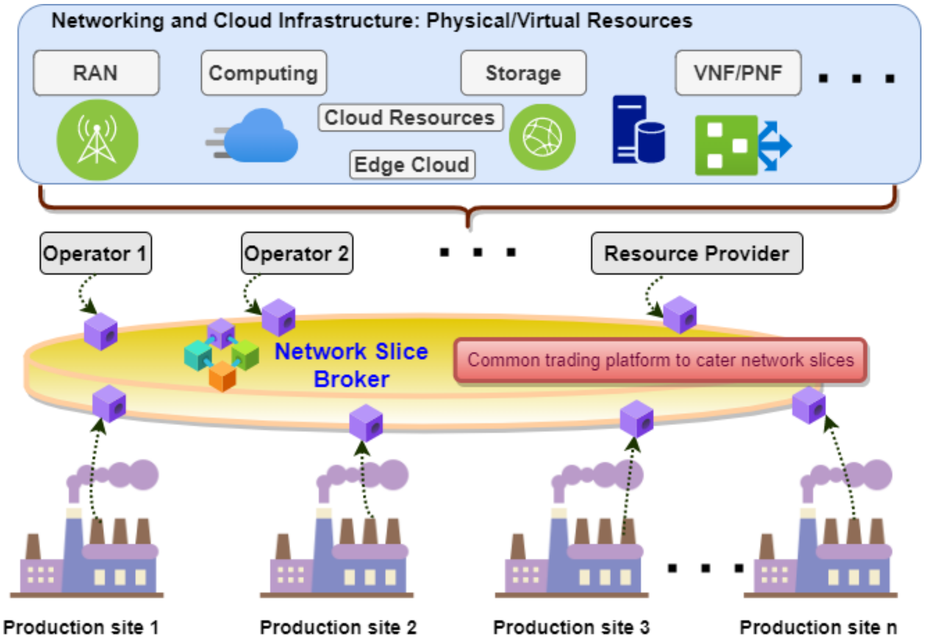

Fig. 9. Role of network slice broker to enable FaaS (Reprinted, with permission, from Paper V © 2022 IEEE).

infrastructure providers willing to trade the resources for the service-oriented factories operating as consumers.

In this experiment, a software program generated a resource request and end-to-end latency measured on each trial for a specific *BlockTime* configuration. It was performed 100 trials for each *BlockTime* configuration and measured the latency on slice selection(brokering) operation, SSLA establishment, and selected federated slice instantiation. The results show that the impact on the *BlockTime* is significantly higher for the slice selection than the SSLA establishment and slice instantiation. The slice brokering operation consists of more block-mining steps in the proposed architecture, including resource request validation, resource offer validation, and selection result validation. Furthermore, SSLA and slice instantiating operations include block mining operations to ensure non-repudiation by maintaining the operation status as blockchain transaction logs. State-of-the-art solutions [169, 185] deliver the network slice as a single commodity that restricts some of the resource providers to cater for the slice requests due to the unavailability of the entire resources required as a single commodity. Incorporation of the slice federation improves the efficiency of resource providers with maximum resource utilization and reduced cost to the consumer. The proposed

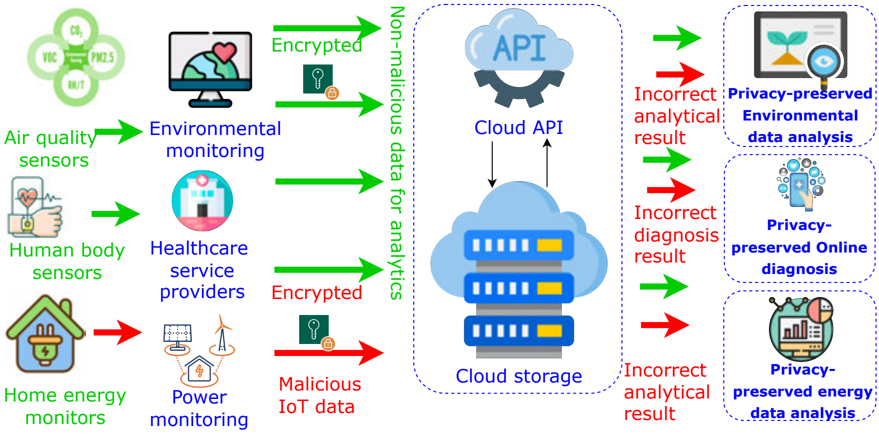
Air quality sensors
Environmental monitoring
Human body sensors
Healthcare service providers
Home energy monitors
Power monitoring
Encrypted
Encrypted
Malicious IoT data
Non-malicious data for analytics
Cloud API
Cloud storage
Incorrect analytical result
Incorrect diagnosis result
Incorrect analytical result
Privacy-preserved Environmental data analysis
Privacy-preserved Online diagnosis
Privacy-preserved energy data analysis

Fig. 10. IoT data formulation systems in industrial applications.

architecture increases the capability of delivering a particular resource request from the available resource providers, defined as the success rate in Paper V. Overall, the proposed architecture ensures lower resource offer pricing compared to the state-of-the-art solutions[169, 185]. Table 3, Table 4, and Table 5 show selected numerical results from the state-of-the-art comparisons.

4.7 Privacy-preserved consensus protocol for reliable IIoT data formulation

4.7.1 Bulletproof based novel privacy-preserved consensus protocol for IoT data formulation

The third research question is focused on efficiently utilizing the reputation score with consensus for reliable IoT data formulation. Figure 10 reflects the IoT data formulation architecture in IoT systems. The security services of the proposed protocol include trusted blockchain node selection through the reputation score and privacy preservation of the reputation score verification to defend against slowly adaptive adversaries. The efficiency features investigated in this research question include energy efficiency and bandwidth utilization efficiency in the privacy-preserved reputation score verification. This proposed consensus protocol enables the incorporation of state-of-the-art domain-specific data validation frameworks such as [87] to evaluate the reputation score based on specific criteria(In [87]-The data range and data sending time profiles are the criteria to distinguish malicious data). However, the state of art reputation score-based consensus protocols[105, 181] are not resistant to slowly adaptive adversaries who were discussed in [130, 218, 129]. Huang et al. [131] proposed to utilize zKSNARK for slowly adaptive adversarial resistant reputation score verification, which incurs an additional overhead of hosting a trusted party to manage keys. However, in the IIoT context, efficiency is vital to improving scalability. Identifying that research gap, the research proposes a novel consensus mechanism utilizing BulletProof[89] that ensures energy and bandwidth consumption efficiency beyond the state of the art by eliminating the energy cost of the trusted third party and shorter messages in the reputation score proof, respectively. Furthermore, the proposed reputation score scheme includes the weighted contribution of a node's waiting time before mining. It outperforms the state-of-the-art reputation score-based consensus protocols[105] with increased fairness between the nodes. The proposed architecture also reduces the waiting time of a node without mining with increased fairness beyond the state of art[105] Table 3, Table 4, and Table 5 show selected numerical results from the state-of-the-art comparisons.

4.8 Security analysis

1. **IoT, Fog, and Cloud node authentication**: The proposed architecture facilitates the ECQV certificate generation and symmetric key establishment as a dynamic operation to minimize the security risk in encryption (symmetric) and authentication (private key of ECQV certificate) key compromise. The valid authentication credential digital certificate has been established with the consensus mechanism with immutable records in the ledger, thereby restricting the identity impersonation to an adversary as defined in RQ1.T1.
2. **Integrity:** The integrity of the key exchange transaction data is ensured in the proposed architecture using the immutable blockchain and integrity-preserved distributed storage (implemented in IPFS). The baseline principle to ensure integrity in blockchain is the digital signature. The blockchain stores the address pointers of the ECQV certificates and hash values generated in Algorithm 2 and Algorithm 3 in Paper II In addition to the digital signatures used in the blockchain, the Schnorr signature scheme has been used to ensure the integrity in messages exchanged between IoT, fog and cloud smart contracts execution. In Paper II, the integration of the Schnorr signature scheme was proposed with decentralized service on smart contracts to defend against manipulations/corruptions of cloud manufacturing instructions/sensor data transferred over the untrusted network as defined in RQ1.T2.

3. **Privacy:** The proposed system ensures privacy in the IoT-CSP channel within the manufacturing process. It is assumed that the IoT-CSP channel will be used to exchange manufacturing-related information and a dynamic session key will be established between IoT and CSP using DH key exchange mechanism and ECIES. Furthermore, the data exchanged within the IoT-Fog-Cloud channel for the session key establishment is encrypted using ECIES to eliminate eavesdropping the sensitive manufacturing instructions/sensor data in IoT-Fog-Cloud channel over the untrusted network as explained in RQ1.T3.
4. **Replay and re-use prevention:** Even though the transaction data preserves anonymity and unlinkability, the data is still verifiable against replay attacks In the proposed architecture, the session counter i is verified at Algorithm 2 using non-interactive ZKP. Furthermore, in Algorithm 2 in Paper II, the ledger is checked for the existence of $primaryHash_i$ in Algorithm 2 and $secondaryHash_i$ in Algorithm 3 in Paper II. Using these techniques and the immutability of the distributed ledger records, the proposed architecture prevents the replay and reuse of authentication credentials as explained in RQ1.T4.
5. **Automated certificate threat scoring and revocation:** The proposed research enables automated threat scoring and certificate revocation using smart contracts. The research leveraged the decentralization and transparency of smart contracts for threat scoring and automated certificate revocation. The consensus-based certificate revocation as an action to the malicious behaviour detected by the IDS ensures that the response is unbiased and based on a transparent evaluation, thereby improving the trust of the entire IIoT system. Furthermore, rather than revocation the certificate based on a binary decision of the IDS, the threat scoring improves the tolerance to false positives, which can be anticipated with the IDS. The automated threat scoring improves threat prioritization and classification capabilities as explained in RQ1.T5.
6. **Anonymity and unlinkability:** Anonymity and unlinkability of the transaction data are ensured using the hashing techniques and non-interactive ZKP in the transaction records. The transaction data which are used in the proposed architecture, including Equation 2 and Table 2(in paper II), do not reveal the identity as well as transaction counter i related information in the ledger records in Paper II. The ledger is completely unaware of the underlying values in the irreversible hash records exchanged in the key certificate activation transactions. Anonymity and unlinkability enable one CSP to facilitate many manufacturing groups, even though each of them is a competitor. Each manufacturing group can integrate into the CM system as a consortium member by connecting the fog computing node. The proposed architecture does not reveal individual transaction information on the blockchain. Using these techniques, the

research enforces anonymity and unlinkability of transaction data as explained in RQ1.T6.

7. **Malicious individual tenants and colluding group detection and prevention of the impact to NSB**: The research proposes to encode individual profiles that define the maximum bounds of network slice requests and resource units to defend the NSB from resource requests which are launched by malicious tenants. The proposed approach restricts the malicious individuals and colluding malicious groups as each type of adversary has to exceed the defined authorized limits of resource units and network slice requests, which is technically impossible. The profile-based restriction of resource requests ensures that the NSB is secured from RQ2.T1 and RQ2.T2.
8. **Malicious individual resource providers and colluding group detection and prevention of the impact to the tenants:** The research proposes to encode individual profiles of the resource providers that define the possible bounds of network slice requests and resource units to deliver for the consumers. At the same time, each has been registered as a resource provider. The proposed approach restricts the malicious resource providers and colluding malicious groups of resource providers as each type of adversary has to align with the defined limits of resource units and network slice requests, which is technically impossible. The profile-based verification of resource offers ensures that the NSB is secured from RQ2.T3 and RQ2.T4.
9. **Transparent and cryptographically integrity-preserved SSLA:** The SSLA defines the specification corresponding to the network slice, including QoS, cryptographic keys, and lifetime of the network slice. The proposed smart contract-based SSLA establishment creates a transparent agreement on SSLa requests with cryptographic integrity preserved digital signatures. The proposed SSLA establishment secures the network slice broker from RQ2.T5.
10. **Elimination of incorrect results of IoT applications from falsified malicious data:** The proposed blockchain-based service architecture enables the domain-specific data validation using data validation smart contracts encoded based on state-of-art IoT data validation frameworks such as [80, 81, 82, 83]. The smart contract guarantees that the data that does not conform to the corresponding data validation framework will not be included in the unmined transaction pool and eventually into the block. The reputation score includes a weighted contribution of data's validity/reliability, which is considered in mining node election according to Equation 9. The RQ3.T1 has been eliminated by filtering out the malicious data based on the validation frameworks and numerically evaluate the trustworthiness and consideration in the mining node election.

11. **Privacy in reputation score verification that improves the resistance to the slowly adaptive adversaries:** In the proposed consensus protocol, the reputation score is shared as a Pedersen commitment without revealing the actual reputation value as indicated in Equation 4 in Paper VI. Using the BulletProof mechanism, the difference between the index and the threshold value can be proven as a positive integer approved in the consensus. Identifying the reputation score from the Pedersen commitment corresponds to the discrete logarithm problem. More specifically, the adversaries cannot identify the reputation score values sc_j and sc_k from the available information tuples $\langle G, H, q, (r_jG + sc_jH) \rangle$ and $\langle G, H, q, (r_kG + sc_kH) \rangle$ when both r_j and r_k values are randomly chosen from a uniform distribution. Thus, information-theoretic privacy is preserved from the perspective of the reputation score. As indicated in Figure 10, the proposed work yields a higher reputation score of the mined blocks than the state-of-the-art when the slowly adaptive adversarial attacks are present. The proposed Pedersen commitment and BulletProofs based method secures the high-reputation mining nodes from the slowly adaptive adversaries, as described in RQ3.T2.
12. **Selfish mining and forking attack:** It can be observed that the chain-length evolution of malicious groups that lead to selfish mining forking attacks and non-malicious groups through programmatic simulation and PAT model checker evaluation. The experimental results reflect that in this thesis, the malicious group cannot chase the non-malicious group in chain growth [219] when the malicious group percentage is less than the percentage required for the consensus. The reputation score of the consensus protocol includes the weighted contribution of criteria that prevents a node from indefinitely waiting for mining, as indicated in Equation 9 of the Paper VI. The reputation scores evolve in the forking attack scenarios without preventing the non-malicious group from mining. Thereby, the chain of blocks of the non-malicious group is always longer than the malicious group's chain length. According to the experimental results portrayed in Figure 13, this research preserves the chain growth up to 5.2 blocks on average, while state-of-the-art chain growth is 1.4 on average for a maximum attack budget is 10 on 100 blockchain nodes.
13. **Mining election disputes:** The proposed protocol identified two potential scenarios for mining election disputes. These dispute scenarios involve two or more mining nodes with a reputation score greater than the threshold value and a mining node claiming the right to replace a mined block due to a delay in claiming the mining qualification. In both cases, the research considered privacy as the primary concern and enabled arbitration mechanisms through smart contracts without revealing the individual reputation score. Algorithm 3 includes the arbitration mechanism

when two or more mining nodes are qualified for mining in a mining call based on the decimal value of the SHA-256 hash. Algorithm 5 handles the arbitration of the second scenario. The proposed mechanisms ensure that the system handles the disputes that occur in the mining process. However, the finalized block from arbitration fulfils the fundamental qualification of exceeding the threshold, which is verified using BulletProof.

14. **Insertion of invalid blocks:** The research defined a block as invalid when the block is not qualified for mining, more specifically when the block is not mined by a node that does not comply with the required reputation score. In the proposed protocol, the reputation score is published as a Pedersen commitment and verified using BulletProof ZKP. The Pedersen commitment for the reputation score is defined as Equation 4 of Paper VI, without the involvement of any trusted setup. Eliminating trusted setup and reputation proof associated with asymmetric keys in this research reduces the risk of fake proofs and invalid blocks preceded with compromised asymmetric keys or trusted setups as proposed in the state of the art [131].
15. **Inconsistency in the ledger:** The research identified that the ledger might cause inconsistency due to a network delay. The arbitration mechanism fixes the blockchain by replacing the qualified block in dispute scenarios using the arbitration smart contract (Algorithm 5 of Paper VI). Eventually, the system reaches a consistent state upon fixing the ledger through arbitration.
16. **Fairness preservation:** The proposed consensus protocol elects the mining nodes based on the reputation score as defined in Equation 9 of the Paper VI. This research considers multiple parameters with weighted contributions in the reputation score evaluation. The reputation score evaluation considers a mining node's last mined time in the reputation score to eliminate a node indefinitely waiting from mining. In the experimental evaluation, the research observed that this thesis enables up to 97.4% of nodes to mine and add a block to the ledger within the experiment, while the implemented state-of-the-art indicated only up to 7.7% nodes enabled for mining, as indicated in Figure 14a in Paper VI while this research indicates up to 19.34% node utilization.

Table 2 reflects a summary of security analysis discussed in Section 4.8.

Table 2. Summary of contributions for security services in the research.

Threat	Summary of contribution in the research
RQ1.T1	IIoT node authentication was performed with ECQV certificates.
RQ1.T2	Digital signature for IIoT-Fog-Cloud messages were used to ensure the integrity of the messages.
RQ1.T3	Diffie-Hellman key exchange for symmetric key establishment between IoT-Fog-Cloud channel.
RQ1.T4	Restricting the number of authentication credentials and key establishments for IoT-Fog-Cloud channel.
RQ1.T5	Smart contracts were used to facilitate trustworthy and transparent threat classification.
RQ1.T6	Formulate the consortium ledger with hash-based records to eliminate linkability.
RQ2.T1	Restricting the tenant resource request and amount of resource units using on-chain profiling for the tenants to limit the malicious attempts to over-utilize the resources in colluding groups with the intention to make the resources unavailable to the legitimate tenants..
RQ2.T2	Restricting the tenant resource request and amount of resource units using on-chain profiling for the tenants to limit the attempts to over-utilize the resources individually to make the resources unavailable to the legitimate tenants.
RQ2.T3	Pre-validation of the resource providers' offers using smart contracts.
RQ2.T4	Ensured non-repudiation with cryptographically integrity-preserved agreement conditions.
RQ3.T1	Validate the data in contrast with state-of-the-art data validation frameworks and formulate the reputation score based on the compliant data.
RQ3.T2	Publishing the reputation score in the form of Pedersen commitments and Bulletproof zero-knowledge proof.

Table 3. Selected numerical results that highlight the advancement of thesis contribution beyond state of the art - RQ1.

Features	State of the art	Thesis result	Remarks
Blockchain storage utilization(RQ1.L1)	3.92 MB [182, 183]	3.13 MB	The results compared when the implementation setup was registered with 10000 IoT nodes. Lower latency indicates the time efficiency in processing certificate credential verification requests.
Authentication service access latency(RQ1.L1)	77.4 ms [217]	22.3 ms	The results compared when the implementation setup was registered with 10000 IoT nodes. Lower latency indicates the time efficiency in processing certificate credential verification requests.
Authentication key size (RQ1.L1)	3072 bit [155]	256 bit	Smaller key sizes enable efficient network utilisation for more IoT nodes to communicate on the existing network resources.

Table 4. Selected numerical results that highlight the advancement of thesis contribution beyond state of the art - RQ2.

Features	State of the art	Thesis result	Remarks
Batched new legitimate slice requests completion latency in attack scenario(RQ2.T1, RQ2.T2, RQ2.T3, RQ2.T4)	34.9 s[185]	6.7 s	The simulated DoS/DDoS attacks affect the slice request completion latency of the legitimate tenants.
Success rate for scaled up resource types (RQ2.L1)	8.3% [169]	96.6%	Success rate for scaled up resource providers
Success rate for scaled-up resource providers(RQ2.L1)	21.3% [185]	97.4%	The proposed architecture enables federated slice formulation that utilizes more resource providers efficiently instead of waiting without slice delivery for the consumer requests.
Resource provider utilization (RQ2.L1, Single slice)	1% [169]	67.4%	The proposed architecture enables federated slice formulation that utilizes more resource providers efficiently instead of waiting without slice delivery for the consumer requests. The result reflects the average contribution of resource providers out of 100 resource providers
Resource offer pricing(RQ2.L1)	4.14 [169]	3.25	Each resource was assigned a numerical cost. The proposed architecture yields lower-cost resource offers with federation of cheaper resource options from multiple resource providers.

Table 5. Selected numerical results that highlight the advancement of thesis contribution beyond state of the art - RQ3.

Features	State of the art	Thesis result	Remarks
Mined block depth (chain growth)in adaptive attacks(RQ3.T2)	1.4 [105]	5.2	The proposed architecture outperforms the preservation of chain growth when compared with the state of art.
Mined node reputation in adaptive attacks(RQ3.T2)	0.74 [105]	0.88	The proposed architecture outperforms a higher average of reputation score in mined nodes when compared with the state of art.
Energy overhead for a mining round(RQ3.L2)	323.4 J[131]	153.3 J	The proposed architecture utilizes BulletProof with improved energy efficiency compared to the state of the art.
Mined node percentage(RQ3.L3)	7.7%[131]	97.4%	The experiment evaluates the node percentage which mined at least one time in a fixed transaction count and fixed number of nodes(results are for 400 nodes and 5000 transactions)
Waiting time as a percentage of experiment time(RQ3.L3)	88.4%[131]	19.34%	The experiment evaluates the node's average waiting time to mine a block as a percentage of experiment time(results are for 400 nodes and 5000 transactions).
Network overhead in mining(RQ3.L3)	10.7 Mb[131]	7.45 Mb	The proposed architecture utilizes BulletProof with shorter proofs compared to the state of art.

5 Discussion

This chapter recaps the thesis. Section 5.1 presents a summary of the contribution of the thesis. Section 5.2 describes the limitations of the proposed work. Section 5.3 proposes the potential future research directions as extensions of the current research. Section 5.4 describes the impact of the research from the perspective of the United Nations(UN) Sustainable Development Goals(SDG).

5.1 Summary of contributions

Authentication, key establishment, secured network slice brokering, and, data formulation are vital services in 5G and beyond connected IIoT networks. IIoT networks are heterogenous with constraints of memory and computational power with the potential to be scaled up. Therefore, efficiency is a vital design consideration. More specifically, the efficiency in network bandwidth consumption, storage utilization, time consumption, and energy consumption are important considerations in the security service design for IIoT.

This thesis presents a high-level overview of the evolution of IIoT and IoT by exploring the potential of blockchain-based smart contracts to develop efficient IIoT security services. From the security perspective, the thesis investigates and proves the potential of blockchain to efficiently facilitate IoT authentication end-to-end key establishment, with anonymity and unlinkability. Paper I utilizes the ECQV certificates for IoT node authentication and automated revocation of certificates for malicious behaviour detection. The implementation results on Raspberry Pi B nodes reflect the deployment capability on IoT nodes. Paper II extends the application of ECQV certificates with smart contracts to automate dynamic certificate generation and IIoT-Fog-Cloud key establishment. Secondly, the thesis investigates the potential of blockchain-based smart contracts to secure the network slice brokering process and propose a decentralized service architecture for secure and efficient network slice brokering. Paper III proposes a blockchain-based IoT tenant and resource provider profiling framework to defend the network slice broker from DoS/DDoS attacks. Paper IV proposes incorporating blockchain and game theory for network federated network slice brokering. Paper V elaborates with blockchain-based network slice brokering to facilitate factory-as-a-service. Finally, Paper VI proposes a novel consensus protocol that utilizes a reputation score mechanism to mining node election and uses BulletProof zero-knowledge proof for reputation score verification to defend the high reputation blockchain nodes from adaptive adversaries. Overall, this thesis provides significant insights into the potential of decentralized service architecture to efficiently secure the 5G and beyond IIoT networks utilizing the smart contract and consensus mechanisms.

In addition to the publications in the thesis, the candidate has published several other research articles in renowned venues by providing the background to the thesis topic. In [106], a comprehensive survey was performed on blockchain-based smart contracts' potential applications and challenges. The article discussed several application domains of blockchain, including finance, telecommunication, manufacturing, and construction with the significant challenges in incorporating blockchain to industrial applications. In [220], a survey was performed on the technical aspects of blockchain-based smart contracts, including the consensus protocols, smart contract types, and potential vulnerabilities. In [221], the role of blockchain in the 5G IoT network was discussed. In [222], the role of blockchain in 6th Generation (6G) networks with potential challenges, opportunities, and research directions was discussed. In [223] , a multi-access edge computing and blockchain-based service architecture was proposed for secured telehealth systems.

5.2 Limitations

The research spanned multiple years, during which the specification of fog computing infrastructure and implemented blockchain platforms evolved with novel advancements. Experimental evaluation on 5G edge infrastructure, such as Nokia OpenEdge, might add more value from the practicality perspective.

The adversaries and attacks defined in Paper I and Paper II need to be aligned with formal attack models such as the Dolev-Yao (D-Y) attack model [191]. It might add value to the research contribution if the designed protocols are verified with a formal verification tool such as Scyther[224] or Avispa[225]. The requirement of blockchain nodes and extended storage has to be deployed. This incurs extra complexity to the infrastructure deployment requirements compared to centralized security service architectures.

In Paper III, additional latency incurred by the smart contract-based verification in the resource request can be identified. However, this latency depends on the block mining interval defined on the security service blockchain. The architecture proposes this, and it can be adjusted via configuration. In Paper IV and Paper V, a blockchain-based network slice brokering framework was proposed. The ledger storage overhead can be identified as a potential limitation against utilizing blockchain. In Paper VI, the overhead of the privacy function can be identified as a potential limitation.

Overall, blockchain is vulnerable to 51% attacks[226]. Furthermore, the resistance of the proposed protocols was not tested from the perspective of the quantum computing evolution[227].

5.3 Future research directions

5.3.1 *Improvements of the current research*

The contributions of Paper I and Paper II must be improved with formal attack modelling and formal verification. In Paper III Paper IV, the storage scalability is one of the features to be improved in the proposed architecture to minimize the impact of the storage overhead. Moreover, the privacy of transaction data, which also provides verifiability in dispute resolution, is a potential future work for Paper III and Paper IV.

5.3.2 *Long-term research objectives*

The long-term research objectives include extending the consensus mechanism of Paper VI to improve the security of federated learning. The objective is to establish a trusted federated learning mechanism with the utilization of consensus protocol.

5.4 Position of the research and the United Nations Sustainable Development Goals

It is important to evaluate the impact of the research on society and the world's sustainability. More specifically, the United Nations Sustainable Development Goals (SDG) is a comprehensive framework that encompasses global challenges, including poverty, inconsistency of healthcare services, climate change, and access restrictions to education [228]. SDG17 includes the officially worded goal to: *Strengthen the means of implementation and revitalize the global partnership for sustainable development*. SDG17.6 highlights the significance of knowledge sharing, and the consensus-based IoT data formulation as proposed in Paper VI is an impactful approach to collaborative and secured data formulation for knowledge sharing. The proposed research ensures the reliability of the data, which eventually converts into knowledge by eliminating the impact of malicious data using the reputation scheme. SDG 9 contains the officially worded goal to:*Build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation*, focusing on innovation, research, and development to drive sustainable industrial growth and technological progress SDG9.1 defines the significance of reliable and sustainable infrastructure that leverages economic development. The research focuses on developing a novel consensus-based federated learning mechanism that increases the reliability of state-of-the-art IIoT systems and improves trust. Furthermore, the research focuses on energy efficiency beyond the state of the art in the proposed consensus mechanism to align with SDG9.4, highlighting clean and environmentally sound technologies. Ultimately, the proposed research ensures a privacy-preserved consensus protocol that ensures the requirements of SDG16, which aims to Promote peaceful and inclusive societies for sustainable development, provide access to justice for all and build effective, accountable and inclusive institutions at all levels. Overall, the proposed research significantly aligns with the SDGs to improve the usability of IIoT with improved privacy, reliability, and reduced energy consumption.

6 Conclusion

Security is a vital requirement in 5G and beyond connected IIoT networks. The IIoT nodes are heterogeneous and require scalability. This research focuses on leveraging decentralized technologies for IIoT.

The thesis commenced by introducing IIoT authentication mechanisms with the significance of designing efficient authentication solutions for IIoT utilizing decentralized technologies. The thesis's first research contribution was exploiting blockchain-based smart contracts to manage ECQV certificates for efficiently authenticating IoT and IoT-Cloud channel privacy. The proposal was extended by enhancing the anonymity and unlinkability of security service-related transactions with extended storage scalability. The security properties, advantages of the storage usage, and latency advantage were evaluated using an experimental implementation setup. Secondly, the research facilitates secured and efficient network slice brokering for multi-tenant and multi-operator scenarios. The second contribution includes incorporating blockchain-based smart contracts to defend the network slice broker from DoS/DDoS attacks. Furthermore, incorporating the Stackalberg game model for federated slice brokering increased the resource provider utilization and provided a cost-effective price to the consumers. The implementation and performance evaluations reflect the advantage of the proposed architecture beyond the state of the art. Finally, this research proposes utilising a consensus mechanism to formulate reliable IoT data. The reputation score was utilized as an indicator to identify the reliability. The proposed solution ensures resistance to the limited budget slowly adaptive attacks targeting the higher mining nodes by integrating BulletProof ZKP for privacy-preserved reputation score verification. The proposed protocol was formally verified for correctness evaluation and benchmarked with several state-of-the-art works to distinguish this thesis's performance and energy advantages. The experimental results yield that the proposed consensus protocol preserves the performance and scalability requirements in 5G connected IoT networks while enforcing the privacy.

Despite the limitations, the results obtained in this thesis show that the proposed decentralized security service architecture is feasible to implement. Finally, the thesis presents insights into emerging future research directions on decentralized machine learning techniques such as federated learning.

References

[1] J. W. Veile, M.-C. Schmidt, and K.-I. Voigt, “Toward a new era of cooperation: How industrial digital platforms transform business models in industry 4.0,” *Journal of Business Research*, vol. 143, pp. 387–405, 2022.

[2] M. Ylianttila, R. Kantola, A. Gurtov, L. Mucchi, I. Oppermann, Z. Yan, T. H. Nguyen, F. Liu, T. Hewa, M. Liyanage *et al.*, “6g white paper: Research challenges for trust, security and privacy,” *arXiv preprint arXiv:2004.11665*, 2020.

[3] A. C. Panchal, V. M. Khadse, and P. N. Mahalle, “Security Issues in IIoT: A Comprehensive Survey of Attacks on IIoT and its Countermeasures,” in *2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN)*. IEEE, 2018, pp. 124–130.

[4] T. Qiu, J. Chi, X. Zhou, Z. Ning, M. Atiquzzaman, and D. O. Wu, “Edge computing in industrial internet of things: Architecture, advances and challenges,” *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2462–2488, 2020.

[5] A. Rahman, M. J. Islam, S. S. Band, G. Muhammad, K. Hasan, and P. Tiwari, “Towards a blockchain-sdn-based secure architecture for cloud computing in smart industrial iot,” *Digital Communications and Networks*, vol. 9, no. 2, pp. 411–421, 2023.

[6] M. Paez and K. Tobitsch, “The industrial internet of things: Risks, liabilities, and emerging legal issues,” *NYL Sch. L. Rev.*, vol. 62, p. 217, 2017.

[7] L. Urquhart and D. McAuley, “Avoiding the internet of insecure industrial things,” *Computer law & security review*, vol. 34, no. 3, pp. 450–466, 2018.

[8] Microsoft, “Azure iot reference architecture,” Tech. Rep., 2023. [Online]. Available: `https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/iot`

[9] IBM, “Ibm, internet of things for insights from connected devices. 2019, available from,” Tech. Rep., 2016. [Online]. Available: `https://www.ibm.com/cloud/architecture/architectures/iotArchitecture`

[10] S. A. Soleymani, S. Goudarzi, M. H. Anisi, H. Cruickshank, A. Jindal, and N. Kama, “Truth: Trust and authentication scheme in 5g-iiot,” *IEEE Transactions on Industrial Informatics*, vol. 19, no. 1, pp. 880–889, 2022.

[11] A. Hazra, M. Adhikari, T. Amgoth, and S. N. Srirama, “A comprehensive survey on interoperability for iiot: taxonomy, standards, and future directions,” *ACM Computing Surveys (CSUR)*, vol. 55, no. 1, pp. 1–35, 2021.

[12] M. Serror, S. Hack, M. Henze, M. Schuba, and K. Wehrle, “Challenges and opportunities in securing the industrial internet of things,” *IEEE Transactions on Industrial Informatics*, vol. 17, no. 5, pp. 2985–2996, 2020.

[13] R. Roman, P. Najera, and J. Lopez, “Securing the internet of things,” *Computer*, vol. 44, no. 9, pp. 51–58, 2011.

[14] C. Shi, Z. Ren, K. Yang, C. Chen, H. Zhang, Y. Xiao, and X. Hou, “Ultra-low latency cloud-fog computing for industrial internet of things,” in *2018 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2018, pp. 1–6.

[15] M. Masdari and M. Jalali, “A survey and taxonomy of dos attacks in cloud computing,” *Security and Communication Networks*, vol. 9, no. 16, pp. 3724–3751, 2016.

[16] S. Nakamoto *et al.*, “Bitcoin: A peer-to-peer electronic cash system,” 2008.

[17] Y. Hao, “Research of the 51% attack based on blockchain,” in *2022 3rd International Conference on Computer Vision, Image and Deep Learning & International Conference on Computer Engineering and Applications (CVIDL & ICCEA)*. IEEE, 2022, pp. 278–283.

[18] N. Alzahrani and N. Bulusu, “A new product anti-counterfeiting blockchain using a truly decentralized dynamic consensus protocol,” *Concurrency and Computation: Practice and Experience*, vol. 32, no. 12, p. e5232, 2020.

[19] V. Dedeoglu, S. Malik, G. Ramachandran, S. Pal, and R. Jurdak, “Blockchain meets edge-ai for food supply chain traceability and provenance,” 2023.

[20] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, “When Mobile Blockchain Meets Edge Computing,” *IEEE Communications Magazine*, vol. 56, no. 8, pp. 33–39, 2018.

[21] S. Panicker, V. Patil, and D. Kulkarni, “An overview of blockchain architecture and it’s applications,” *International Journal of Innovative Research in Science, Engineering and Technology*, vol. 5, no. 11, pp. 1111–1125, 2016.

[22] C. Bormann, M. Ersue, A. Keranen *et al.*, “Architecture for the Internet of Things: RFC 7452,” Internet Engineering Task Force, RFC 7452, March 2015. [Online]. Available: https://tools.ietf.org/html/rfc7452

[23] P. Fremantle *et al.*, “A reference architecture for the internet of things,” *WSO2 White paper*, pp. 02–04, 2015.

[24] I. I. Consortium, “Industrial internet reference architecture,” Tech. Rep., 2015. [Online]. Available: https://www.iiconsortium.org/pdf/IIC_PUB_G1_V1.80_2017-01-31.pdf

[25] T. O. Group, “Open platform 3.0™ architecture,” Tech. Rep., 2014. [Online]. Available: https://www.opengroup.org/public/arch/p3/TOGAF_OP3_Standard_v1.0.pdf

[26] M. Centenaro, L. Vangelista, A. Zanella, and M. Zorzi, “Long-range communications in unlicensed bands: The rising stars in the IoT and smart city scenarios,” *IEEE Wireless Communications*, vol. 23, no. 5, pp. 60–67, Oct. 2016.

[27] Zigbee Alliance, “Zigbee specification,” Online, Sep. 2021. [Online]. Available: https://zigbeealliance.org/wp-content/uploads/2021/09/docs-05-3474-21-0csg-zigbee-specification.pdf

[28] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, “The industrial internet of things (iiot): An analysis framework,” *Computers in industry*, vol. 101, pp. 1–12, 2018.

[29] W. Z. Khan, M. Rehman, H. M. Zangoti, M. K. Afzal, N. Armi, and K. Salah, “Industrial internet of things: Recent advances, enabling technologies and open challenges,” *Computers & electrical engineering*, vol. 81, p. 106522, 2020.

[30] L. Da Xu, W. He, and S. Li, “Internet of Things in Industries: A Survey,” *IEEE Transactions on industrial informatics*, vol. 10, no. 4, pp. 2233–2243, 2014.

[31] S. D. Milić and B. M. Babić, “Toward the future—upgrading existing remote monitoring concepts to iiot concepts,” *IEEE Internet of Things Journal*, vol. 7, no. 12, pp. 11 693–11 700, 2020.

[32] X. Huang, “Intelligent remote monitoring and manufacturing system of production line based on industrial internet of things,” *Computer Communications*, vol. 150, pp. 421–428, 2020.

[33] C. Xiang and B. Li, “Research on ship intelligent manufacturing data monitoring and quality control system based on industrial internet of things,” *The International Journal of Advanced Manufacturing Technology*, vol. 107, pp. 983–992, 2020.

[34] L. Haghnegahdar, S. S. Joshi, and N. B. Dahotre, “From iot-based cloud manufacturing approach to intelligent additive manufacturing: Industrial internet of things—an overview,” *The International Journal of Advanced Manufacturing Technology*, pp. 1–18, 2022.

[35] M. S. Hossain and G. Muhammad, “Cloud-assisted industrial internet of things (iiot)–enabled framework for health monitoring,” *Computer Networks*, vol. 101, pp. 192–202, 2016.

[36] S. Iranpak, A. Shahbahrami, and H. Shakeri, “Remote patient monitoring and classifying using the internet of things platform combined with cloud computing,” *Journal of Big Data*, vol. 8, pp. 1–22, 2021.

[37] A. Zhang and K. Zhang, “Enabling Concurrency on Smart Contracts using Multiversion Ordering,” in *Asia-Pacific Web (APWeb) and Web-Age Information Management (WAIM) Joint International Conference on Web and Big Data*. Springer, 2018, pp. 425–439.

[38] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, “Consortium blockchain for secure energy trading in industrial internet of things,” *IEEE transactions on industrial informatics*, vol. 14, no. 8, pp. 3690–3700, 2017.

[39] P. Asef, R. Taheri, M. Shojafar, I. Mporas, and R. Tafazolli, “Siems: A secure intelligent energy management system for industrial iot applications,” *IEEE Transactions on Industrial Informatics*, vol. 19, no. 1, pp. 1039–1050, 2022.

[40] S. Malik, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, “Trustchain: Trust management in blockchain and iot supported supply chains,” in *2019 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 2019, pp. 184–193.

[41] “characterization of cyber-physical sensor systems.”

[42] Y. Lu and F. Ju, “Smart Manufacturing Systems based on Cyber-physical Manufacturing services (CPMS),” *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 15 883–15 889, 2017.

[43] A. Ren, D. Wu, W. Zhang, J. Terpenny, and P. Liu, “Cyber Security in Smart Manufacturing: Survey and Challenges,” in *IIE Annual Conference. Proceedings*. Institute of Industrial and Systems Engineers (IISE), 2017, pp. 716–721.

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

[45] K. Tange, M. De Donno, X. Fafoutis, and N. Dragoni, “A systematic survey of industrial internet of things security: Requirements and fog computing opportunities,” *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2489–2520, 2020.

[46] X. Yu and H. Guo, “A survey on iiot security,” in *2019 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS)*. IEEE, 2019, pp. 1–5.

[47] K. Tsiknas, D. Taketzis, K. Demertzis, and C. Skianis, “Cyber threats to industrial iot: a survey on attacks and countermeasures,” *IoT*, vol. 2, no. 1, pp. 163–186, 2021.

[48] I. O. for Standardization, “Information technology - security techniques - information security management systems - requirements,” International Organization for Standardization, Technical Report 27001, 2013. [Online]. Available: `https://www.iso.org/standard/54534.html`

[49] I. E. Commission, “Industrial communication networks - network and system security - part 1-4: Security requirements for components and systems,” International Electrotechnical Commission, Technical Report 62443-1-4, 2018. [Online]. Available: `https://webstore.iec.ch/publication/32349`

[50] N. I. of Standards and Technology, “Framework for improving critical infrastructure cybersecurity,” National Institute of Standards and Technology, Technical Report NIST CSF, 2018. [Online]. Available: `https://www.nist.gov/publications/framework-improving/-critical-infrastructure-cybersecurity`

[51] National Institute of Standards and Technology (NIST), “Protecting the nation’s critical infrastructure: National cybersecurity framework,” U.S. Department of Commerce, Technical Report, 2014. [Online]. Available: `https://www.nist.gov/cyberframework`

[52] M. Shafique, T. Theocharides, C.-S. Bouganis, M. A. Hanif, F. Khalid, R. Hafız, and S. Rehman, “An overview of next-generation architectures for machine learning: Roadmap,

opportunities and challenges in the iot era," in *2018 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 2018, pp. 827–832.

[53] H. Jayakumar, A. Raha, Y. Kim, S. Sutar, W. S. Lee, and V. Raghunathan, "Energy-efficient system design for iot devices," in *2016 21st Asia and South Pacific design automation conference (ASP-DAC)*. IEEE, 2016, pp. 298–301.

[54] H. Rafiq, N. Aslam, U. Ahmed, and J. C.-W. Lin, "Mitigating malicious adversaries evasion attacks in industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 1, pp. 960–968, 2022.

[55] J. Daubert, A. Wiesmaier, and P. Kikiras, "A view on privacy & trust in iot," in *2015 IEEE International Conference on Communication Workshop (ICCW)*. IEEE, 2015, pp. 2665–2670.

[56] G. Fortino, L. Fotia, F. Messina, D. Rosaci, and G. M. Sarné, "Trust and reputation in the internet of things: State-of-the-art and research challenges," *IEEE Access*, vol. 8, pp. 60 117–60 125, 2020.

[57] A. Mahmood, L. Beltramelli, S. F. Abedin, S. Zeb, N. I. Mowla, S. A. Hassan, E. Sisinni, and M. Gidlund, "Industrial iot in 5g-and-beyond networks: Vision, architecture, and design trends," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 6, pp. 4122–4137, 2021.

[58] S. Eswaran and P. Honnavalli, "Private 5g networks: a survey on enabling technologies, deployment models, use cases and research directions," *Telecommunication Systems*, vol. 82, no. 1, pp. 3–26, 2023.

[59] M. M. Hassan, A. Abdulla, W. Ahmed, M. A. Ahmed, and M. M. Hossain, "A survey of 5g network: architecture and emerging technologies," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–29, 2021.

[60] R. Abbas, W. Zhang, I. Yaqoob, M. A. Imran, M.-S. Alouini, and S. Chen, "5g and industrial internet of things revolution," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3665–3673, 2019.

[61] F. Hussain, K. Salah, Z. Abdelouahab, and F. Al-Turjman, "5g wireless networks: Opportunities and challenges for the industrial internet of things," *IEEE Communications Magazine*, vol. 56, no. 6, pp. 21–27, 2018.

[62] M. H. Islam, M. S. Biswas, X. Li, Y. Zhang, and X. Liang, "5g-enabled industrial internet of things: Security and privacy challenges, and solutions," *IEEE Communications Magazine*, vol. 57, no. 8, pp. 46–51, 2019.

[63] R. Jiang, J. Chen, H. Yu, Y. Zhang, Z. Xu, and R. Huang, "Secure 5g-enabled internet of things for industrial automation: Challenges and solutions," *IEEE Communications Magazine*, vol. 58, no. 1, pp. 34–41, 2020.

[64] K. Zhang, T. Liang, Y. Li, Z. Zhang, and W. Wang, "5g-enabled industrial internet of things: Vision, requirements, and challenges," *IEEE Wireless Communications*, vol. 27, no. 4, pp. 124–130, 2020.

[65] "An introduction to network slicing," GSMA Network Tech. Report, 2017, accessed on 15.01.2021. [Online]. Available: `https://www.gsma.com/futurenetworks/wp-content/uploads/2017/11//GSMA-An-Introduction-to-Network-Slicing.pdf`

[66] S. Wijethilaka and M. Liyanage, "Survey on Network Slicing for Internet of Things Realization in 5g Networks," *IEEE Communications Surveys & Tutorials*, 2021.

[67] S. Kukliński, L. Tomaszewski, K. Kozłowski, and S. Pietrzyk, "Business models of network slicing," in *2018 9th International Conference on the Network of the Future (NOF)*. IEEE, 2018, pp. 39–43.

[68] A. Antonopoulos, "Bankruptcy Problem in Network Sharing: Fundamentals, Applications and Challenges," *IEEE Wireless Communications*, vol. 27, no. 4, pp. 81–87, 2020.

[69] K. Samdanis, X. Costa-Perez, and V. Sciancalepore, "From network sharing to multi-tenancy: The 5G network slice broker," *IEEE Communications Magazine*, vol. 54, no. 7, pp. 32–39, 2016.

[70] V. A. Cunha, E. da Silva, M. B. de Carvalho, D. Corujo, J. P. Barraca, D. Gomes, L. Z. Granville, and R. L. Aguiar, "Network Slicing Security: Challenges and Directions," *Internet Technology Letters*, vol. 2, no. 5, p. e125, 2019.

[71] P. Porambage, Y. Miche, A. Kalliola, M. Liyanage, and M. Ylianttila, "Secure keying scheme for network slicing in 5g architecture," in *2019 IEEE Conference on Standards for Communications and Networking (CSCN)*. IEEE, 2019, pp. 1–6.

[72] D. Sattar and A. Matrawy, "Towards Secure Slicing: Using Slice Isolation to Mitigate DDoS Attacks on 5G Core Network Slices," in *2019 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2019, pp. 82–90.

[73] A. S. Mamolar, Z. Pervez, J. M. A. Calero, and A. M. Khattak, "Towards the Transversal Detection of DDoS Network Attacks in 5G Multi-tenant Overlay Networks," *Computers & Security*, vol. 79, pp. 132–147, 2018.

[74] H. Moudoud, L. Khoukhi, and S. Cherkaoui, "Prediction and detection of fdia and ddos attacks in 5g enabled iot," *IEEE Network*, 2020.

[75] K. Lalropuia and V. Gupta, "A Bayesian Game Model and Network Availability Model for Small Cells under Denial of Service (DoS) Attack in 5G Wireless Communication Network," *Wireless Networks*, vol. 26, no. 1, pp. 557–572, 2020.

[76] M. Latva-aho, K. Leppänen, F. Clazzer, and A. Munari, "Key drivers and research challenges for 6g ubiquitous wireless intelligence," 2020.

[77] T. Hewa, G. Gür, A. Kalla, M. Ylianttila, A. Bracken, and M. Liyanage, "The role of blockchain in 6G: Challenges, opportunities and research directions," in *2020 2nd 6G Wireless Summit (6G SUMMIT)*. IEEE, 2020, pp. 1–5.

[78] S. Dang, O. Amin, B. Shihada, and M.-S. Alouini, "What should 6g be?" *Nature Electronics*, vol. 3, no. 1, pp. 20–29, 2020.

[79] M. Z. Khan, O. H. Alhazmi, M. A. Javed, H. Ghandorh, and K. S. Aloufi, "Reliable internet of things: Challenges and future trends," *Electronics*, vol. 10, no. 19, p. 2377, 2021.

[80] N. A. M. Alduais, J. Abdullah, A. Jamil, L. Audah, and R. Alias, "Sensor Node Data Validation Techniques for Realtime IoT/WSN Application," in *2017 14th International Multi-Conference on Systems, Signals & Devices (SSD)*. IEEE, 2017, pp. 760–765.

[81] F. Hussain, S. G. Abbas, G. A. Shah, I. M. Pires, U. U. Fayyaz, F. Shahzad, N. M. Garcia, and E. Zdravevski, "A Framework for Malicious Traffic Detection in IoT Healthcare Environment," *Sensors*, vol. 21, no. 9, p. 3025, 2021.

[82] B. Ačko, H. Weber, D. Hutzschenreuter, and I. Smith, "Communication and Validation of Metrological Smart Data in IoT-networks." *Advances in Production Engineering & Management*, vol. 15, no. 1, 2020.

[83] H. Sándor, B. Genge, and Z. Szántó, "Sensor Data Validation and Abnormal Behavior Detection in the Internet of Things," in *2017 16th RoEduNet Conference: Networking in Education and Research (RoEduNet)*. IEEE, 2017, pp. 1–5.

[84] H. Deng, Z. Qin, L. Sha, and H. Yin, "A Flexible Privacy-preserving Data Sharing Scheme in Cloud-assisted IoT," *IEEE Internet of Things Journal*, vol. 7, no. 12, pp. 11 601–11 611, 2020.

[85] R. Tso, A. Alelaiwi, S. M. Mizanur Rahman, M.-E. Wu, and M. S. Hossain, "Privacy-preserving Data Communication through Secure Multi-party Computation in Healthcare Sensor Cloud," *Journal of Signal Processing Systems*, vol. 89, no. 1, pp. 51–59, 2017.

[86] S. Sharma, K. Chen, and A. Sheth, “Toward Practical Privacy-preserving Analytics for IoT and Cloud-based Healthcare Systems,” *IEEE Internet Computing*, vol. 22, no. 2, pp. 42–51, 2018.

[87] D. Li, X. Liao, T. Xiang, J. Wu, and J. Le, “Privacy-preserving self-serviced medical diagnosis scheme based on secure multi-party computation,” *Computers & Security*, vol. 90, p. 101701, 2020.

[88] Z. Guan, Y. Zhang, L. Wu, J. Wu, J. Li, Y. Ma, and J. Hu, “APPA: An Anonymous and Privacy preserving Data Aggregation Scheme for Fog-enhanced IoT,” *Journal of Network and Computer Applications*, vol. 125, pp. 82–92, 2019.

[89] B. Bünz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, and G. Maxwell, “Bulletproofs: Short proofs for Confidential Transactions and More,” in *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2018, pp. 315–334.

[90] M. Liyanage, I. Ahmad, A. B. Abro, A. Gurtov, and M. Ylianttila, *A Comprehensive Guide to 5G Security*. John Wiley & Sons, 2018.

[91] W. Al-Saqaf and N. Seidler, “Blockchain Technology for Social Impact: Opportunities and Challenges Ahead,” *Journal of Cyber Policy*, vol. 2, no. 3, pp. 338–354, 2017.

[92] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, “Bubbles of Trust: A Decentralized Blockchain-based Authentication System for IoT,” *Computers & Security*, vol. 78, pp. 126–142, 2018.

[93] I. Mistry, S. Tanwar, S. Tyagi, and N. Kumar, “Blockchain for 5G-enabled IoT for Industrial Automation: A Systematic Review, Solutions, and Challenges,” *Mechanical Systems and Signal Processing*, vol. 135, p. 106382, 2020.

[94] K. Wang, Y. Wang, and Z. Ji, “Defending blockchain forking attack by delaying mtc confirmation,” *IEEE Access*, vol. 8, pp. 113 847–113 859, 2020.

[95] G. D. Putrat, S. Malik, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, “Trust and reputation management for blockchain-enabled iot,” in *2023 15th International Conference on COMmunication Systems & NETworkS (COMSNETS)*. IEEE, 2023, pp. 529–536.

[96] M. Pilkington, “Blockchain technology: principles and applications,” in *Research handbook on digital transformations*. Edward Elgar Publishing, 2016.

[97] M. J. M. Chowdhury, A. Colman, M. A. Kabir, J. Han, and P. Sarda, “Blockchain versus Database: A Critical Analysis,” in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. IEEE, 2018, pp. 1348–1353.

[98] F. Hofmann, S. Wurster, E. Ron, and M. Böhmecke-Schwafert, “The immutability concept of blockchains and benefits of early standardization,” in *2017 ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K)*. IEEE, 2017, pp. 1–8.

[99] M. Di Pierro, “What is the Blockchain?” *Computing in Science & Engineering*, vol. 19, no. 5, pp. 92–95, 2017.

[100] A. Anjum, M. Sporny, and A. Sill, “Blockchain standards for compliance and trust,” *IEEE Cloud Computing*, vol. 4, no. 4, pp. 84–90, 2017.

[101] A. Singh, G. Kumar, R. Saha, M. Conti, M. Alazab, and R. Thomas, “A survey and taxonomy of consensus protocols for blockchains,” *Journal of Systems Architecture*, p. 102503, 2022.

[102] S. Zhang and J.-H. Lee, “Analysis of the main consensus protocols of blockchain,” *ICT express*, vol. 6, no. 2, pp. 93–97, 2020.

[103] G. Wood, “Ethereum: A Secure Decentralised Generalised Transaction Ledger,” *Ethereum project yellow paper*, vol. 151, pp. 1–32, 2014.

[104] H. Fabric, “Hyperledger Fabric,” *https://www.hyperledger.org/wp-content/uploads/2018/07/*, 2018.

[105] J. Yang, M. M. H. Onik, N.-Y. Lee, M. Ahmed, and C.-S. Kim, “Proof-of-Familiarity: A Privacy-Preserved Blockchain Scheme for Collaborative Medical Decision-Making,” *Applied Sciences*, vol. 9, no. 7, p. 1370, 2019.

[106] T. Hewa, M. Ylianttila, and M. Liyanage, “Survey on blockchain based smart contracts: Applications, opportunities and challenges,” *Journal of network and computer applications*, vol. 177, p. 102857, 2021.

[107] N. Reiff, “What Is ERC-20 and What Does It Mean for Ethereum?” 2020. [Online]. Available: `https://www.investopedia.com/news/what-erc20-and-what-does-it-mean-ethereum/`

[108] Z. Zheng, S. Xie, H.-N. Dai, W. Chen, X. Chen, J. Weng, and M. Imran, “An Overview on Smart Contracts: Challenges, Advances and Platforms,” *Future Generation Computer Systems*, vol. 105, pp. 475–491, 2020.

[109] I. Bashir, *Mastering Blockchain: Distributed Ledger Technology, Decentralization, and Smart Contracts Explained*. Packt Publishing Ltd, 2018.

[110] D. Macrinici, C. Cartofeanu, and S. Gao, “Smart Contract Applications within Blockchain Technology: A Systematic Mapping Study,” *Telematics and Informatics*, 2018.

[111] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An Overview of Blockchain Technology: Architecture, consensus, and Future Trends,” in *2017 IEEE international congress on big data (BigData congress)*. IEEE, 2017, pp. 557–564.

[112] A. Norta, “Designing a Smart-contract Application Layer for Transacting Decentralized Autonomous Organizations,” in *International Conference on Advances in Computing and Data Sciences*. Springer, 2016, pp. 595–604.

[113] T. Mancini-Griffoli, M. S. M. Peria, I. Agur, A. Ari, J. Kiff, A. Popescu, and C. Rochon, “Casting Light on Central Bank Digital Currency,” *IMF Staff Discussion Notes*, no. 18-08, 2018.

[114] E. Shapiro, “Point: Foundations of e-democracy,” *Communications of the ACM*, vol. 61, no. 8, pp. 31–34, 2018.

[115] S. S. Gupta, *Blockchain*. John Wiley & Sons, Inc, 2017.

[116] F. Rizal Batubara, J. Ubacht, and M. Janssen, “Unraveling transparency and accountability in blockchain,” in *Proceedings of the 20th Annual International Conference on Digital Government Research*, 2019, pp. 204–213.

[117] T. Nugent, D. Upton, and M. Cimpoesu, “Improving Data Transparency in Clinical Trials using Blockchain Smart Contracts,” *F1000Research*, vol. 5, 2016.

[118] F. Yiannas, “A New Era of Food Transparency Powered by Blockchain,” *Innovations: Technology, Governance, Globalization*, vol. 12, no. 1-2, pp. 46–56, 2018.

[119] M. Farnaghi and A. Mansourian, “Blockchain, an enabling technology for transparent and accountable decentralized public participatory gis,” *Cities*, vol. 105, p. 102850, 2020.

[120] N. Pokrovskaia, “Tax, financial and social regulatory mechanisms within the knowledge-driven economy. blockchain algorithms and fog computing for the efficient regulation,” in *2017 XX IEEE International Conference on Soft Computing and Measurements (SCM)*. IEEE, 2017, pp. 709–712.

[121] F. Sander, J. Semeijn, and D. Mahr, “The acceptance of blockchain technology in meat traceability and transparency,” *British Food Journal*, 2018.

[122] A. H. Lone and R. Naaz, “Applicability of blockchain smart contracts in securing internet and iot: A systematic literature review,” *Computer Science Review*, vol. 39, p. 100360, 2021.

[123] N. Fotiou and G. C. Polyzos, “Smart Contracts for the Internet of Things: Opportunities and Challenges,” in *2018 European Conference on Networks and Communications (EuCNC)*. IEEE, 2018, pp. 256–260.

[124] V. Buterin *et al.*, “A Next-generation Smart Contract and Decentralized Application Platform,” *white paper*, vol. 3, p. 37, 2014.

[125] W. Corda, “Corda Technical Whitepaper,” *https://www.corda.net/content/corda-technical-whitepaper.pdf.*

[126] C. Khan, A. Lewis, E. Rutland, C. Wan, K. Rutter, and C. Thompson, “A distributed-ledger consortium model for collaborative innovation,” *Computer*, vol. 50, no. 9, pp. 29–37, 2017.

[127] R. Lu, K. Heung, A. H. Lashkari, and A. A. Ghorbani, “A Lightweight Privacy-preserving Data Aggregation Scheme for Fog Computing-enhanced IoT,” *IEEE access*, vol. 5, pp. 3302–3312, 2017.

[128] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, “EPPA: An Efficient and Privacy-preserving Aggregation Scheme for Secure Smart Grid Communications,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1621–1631, 2012.

[129] A. Kiayias, A. Russell, B. David, and R. Oliynykov, “Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol,” in *Annual international cryptology conference*. Springer, 2017, pp. 357–388.

[130] M. Zamani, M. Movahedi, and M. Raykova, “Rapidchain: Scaling Blockchain via Full Sharding,” in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2018, pp. 931–948.

[131] C. Huang, Y. Zhao, H. Chen, X. Wang, Q. Zhang, Y. Chen, H. Wang, and K.-Y. Lam, “ZkRep: A Privacy-Preserving Scheme for Reputation-Based Blockchain System,” *IEEE Internet of Things Journal*, vol. 9, no. 6, pp. 4330–4342, 2021.

[132] M. Aazam, S. Zeadally, and K. A. Harras, “Deploying fog computing in industrial internet of things and industry 4.0,” *IEEE Transactions on Industrial Informatics*, vol. 14, no. 10, pp. 4674–4682, 2018.

[133] F. T. Q.Li, “A Smart Manufacturing Service System Based on Edge Computing, Fog Computing, and Cloud Computing,” *IEEE Access, 7, pp 86769 - 86777, 2019*, 2019.

[134] M. Liyanage, A. Braeken, P. Kumar, and M. Ylianttila, *IoT Security: Advances in Authentication*. John Wiley & Sons, 2020.

[135] P. Wang, R. X. Gao, and Z. Fan, “Cloud computing for cloud manufacturing: benefits and limitations,” *Journal of Manufacturing Science and Engineering*, vol. 137, no. 4, 2015.

[136] R. Henzel and G. Herzwurm, “Cloud Manufacturing: A state-of-the-art Survey of Current Issues,” *Procedia CIRP*, vol. 72, pp. 947–952, 2018.

[137] S. D. C. Avasalcai, I. Murturi, “Edge and Fog: A Survey, use cases, and Future Challenges ,” *Wiley, ISBN 9781119551690, 2020*, 2020.

[138] S. Patonico, A. Braeken, and K. Steenhaut, “Identity-based and Anonymous Key Agreement Protocol for Fog Computing Resistant in the Canetti–Krawczyk Security Model,” *Wireless Networks*, pp. 1–13, 2019.

[139] S. Sciancalepore, A. Capossele, G. Piro, G. Boggia, and G. Bianchi, “Key Management Protocol with Implicit Certificates for IoT Systems,” in *Proceedings of the 2015 Workshop on IoT challenges in Mobile and Industrial Systems*, 2015, pp. 37–42.

[140] P. Fremantle, B. Aziz, J. Kopeckỳ, and P. Scott, “Federated identity and access management for the internet of things,” in *2014 International Workshop on Secure Internet of Things*. IEEE, 2014, pp. 10–17.

[141] S. Cantor and T. Scavo, “Shibboleth architecture,” *Protocols and Profiles*, vol. 10, no. 16, p. 29, 2005.

[142] M. Dammak, S.-M. Senouci, M. A. Messous, M. H. Elhdhili, and C. Gransart, "Decentralized lightweight group key management for dynamic access control in iot environments," *IEEE Transactions on Network and Service Management*, vol. 17, no. 3, pp. 1742–1757, 2020.

[143] M. R. Abdmeziem, D. Tandjaoui, and I. Romdhani, "A decentralized batch-based group key management protocol for mobile internet of things (dbgk)," in *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing*. IEEE, 2015, pp. 1109–1117.

[144] R. Kumar, S. K. Singh, D. Lobiyal, K. T. Chui, D. Santaniello, and M. K. Rafsanjani, "A novel decentralized group key management scheme for cloud-based vehicular iot networks," *International Journal of Cloud Applications and Computing (IJCAC)*, vol. 12, no. 1, pp. 1–34, 2022.

[145] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. Tygar, "Spins: Security protocols for sensor networks," in *Proceedings of the 7th annual international conference on Mobile computing and networking*, 2001, pp. 189–199.

[146] T. Hewa, A. Kalla, A. Nag, M. Ylianttila, and M. Liyanage, "Blockchain for 5G and IoT: Opportunities and Challenges," in *The 8th IEEE International Conference on Communications and Networkinbg (IEEE COMNET'2020)*, Hammamet, Tunisia, 03 2020.

[147] O. Bouachir, M. Aloqaily, L. Tseng, and A. Boukerche, "Blockchain and Fog Computing for Cyberphysical Systems: The Case of Smart Industry," *Computer*, vol. 53, no. 9, pp. 36–45, 2020.

[148] T. R. Gadekallu, Q.-V. Pham, D. C. Nguyen, P. K. R. Maddikunta, N. Deepa, B. Prabadevi, P. N. Pathirana, J. Zhao, and W.-J. Hwang, "Blockchain for Edge of Things: Applications, Opportunities, and Challenges," *IEEE Internet of Things Journal*, 2021.

[149] U. Bodkhe, S. Tanwar, K. Parekh, P. Khanpara, S. Tyagi, N. Kumar, and M. Alazab, "Blockchain for Industry 4.0: A Comprehensive Review," *IEEE Access*, vol. 8, pp. 79 764–79 800, 2020.

[150] T. M. Fernandez-Carames and P. Fraga-Lamas, "A Review on the Application of Blockchain to the Next Generation of cybersecure Industry 4.0 Smart Factories," *IEEE Access*, vol. 7, pp. 45 201–45 218, 2019.

[151] N. Mohamed and J. Al-Jaroodi, "Applying blockchain in industry 4.0 applications," in *2019 IEEE 9th annual computing and communication workshop and conference (CCWC)*. IEEE, 2019, pp. 0852–0858.

[152] F. L. M. Ma, G. Shi, "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT ," *IEEE journal of Internet of Things, 14(8), pp. 1184-1195, 2018*, 2018.

[153] Y. Zhang, X. Xu, A. Liu, Q. Lu, L. Xu, and F. Tao, "Blockchain-based Trust Mechanism for IoT-based Smart Manufacturing System," *IEEE Transactions on Computational Social Systems*, vol. 6, no. 6, pp. 1386–1394, 2019.

[154] S. B. ElMamy, H. Mrabet, H. Gharbi, A. Jemai, and D. Trentesaux, "A Survey on the Usage of Blockchain Technology for Cyber-threats in the Context of Industry 4.0," *Sustainability*, vol. 12, no. 21, p. 9179, 2020.

[155] M. Shen, H. Liu, L. Zhu, K. Xu, H. Yu, X. Du, and M. Guizani, "Blockchain-assisted Secure Device Authentication for Cross-domain Industrial IoT," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 5, pp. 942–954, 2020.

[156] A. B. P. Shabisha, K. Steenhaut, "Anonymous Symmetric Key Based Key Agreement Protocol for Fog Computing," *IEEE IoT Journal*.

[157] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "LSB: A Lightweight Scalable Blockchain for IoT Security and Anonymity," *Journal of Parallel and Distributed Computing*, vol. 134, pp. 180–197, 2019.

[158] T. Kumar, E. Harjula, M. Ejaz, A. Manzoor, P. Porambage, I. Ahmad, M. Liyanage, A. Braeken, and M. Ylianttila, "BlockEdge: Blockchain-edge Framework for Industrial IoT Networks," *IEEE Access*, vol. 8, pp. 154 166–154 185, 2020.

[159] W. Wang, H. Xu, M. Alazab, T. R. Gadekallu, Z. Han, and C. Su, "Blockchain-Based Reliable and Efficient Certificateless Signature for IIoT Devices," *IEEE Transactions on Industrial Informatics*, 2021.

[160] A. Singla and E. Bertino, "Blockchain-based pki solutions for iot," in *2018 IEEE 4th international conference on collaboration and internet computing (CIC)*. IEEE, 2018, pp. 9–15.

[161] B. Qin, J. Huang, Q. Wang, X. Luo, B. Liang, and W. Shi, "Cecoin: A decentralized pki mitigating mitm attacks," *Future Generation Computer Systems*, vol. 107, pp. 805–815, 2020.

[162] A. Yakubov, W. Shbair, A. Wallbom, D. Sanda *et al.*, "A blockchain-based pki management framework," in *The First IEEE/IFIP International Workshop on Managing and Managed by Blockchain (Man2Block) colocated with IEEE/IFIP NOMS 2018, Tapei, Tawain 23-27 April 2018*, 2018.

[163] A. Boubendir, F. Guillemin, C. Le Toquin, M.-L. Alberi-Morel, F. Faucheux, S. Kerboeuf, J.-L. Lafragette, and B. Orlandi, "Federation of cross-domain edge resources: A brokering architecture for network slicing," in *2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft)*. IEEE, 2018, pp. 415–423.

[164] V. Sciancalepore, L. Zanzi, X. Costa-Perez, and A. Capone, "Onets: Online network slice broker from theory to practice," *IEEE Transactions on Wireless Communications*, vol. 21, no. 1, pp. 121–134, 2021.

[165] R. Swami, M. Dave, and V. Ranga, "Software-defined Networking-based DDoS Defense Mechanisms," *ACM Computing Surveys (CSUR)*, vol. 52, no. 2, pp. 1–36, 2019.

[166] J. Backman, S. Yrjölä, K. Valtanen, and O. Mämmelä, "Blockchain network slice broker in 5G: Slice leasing in factory of the future use case," in *2017 Internet of Things Business Models, Users, and Networks*. IEEE, 2017, pp. 1–8.

[167] K. Valtanen, J. Backman, and S. Yrjölä, "Creating value through blockchain powered resource configurations: Analysis of 5G network slice brokering case," in *2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*. IEEE, 2018, pp. 185–190.

[168] N. Afraz and M. Ruffini, "5G network slice brokering: A distributed blockchain-based market," in *2020 European Conference on Networks and Communications (EuCNC)*. IEEE, 2020, pp. 23–27.

[169] L. Zanzi, A. Albanese, V. Sciancalepore, and X. Costa-Pérez, "NSBchain: A secure blockchain framework for network slicing brokerage," in *IEEE International Conference on Communications (ICC)*, 2020, pp. 1–7.

[170] B. Nour, A. Ksentini, N. Herbaut, P. A. Frangoudis, and H. Moungla, "A blockchain-based network slice broker for 5G services," *IEEE Networking Letters*, vol. 1, no. 3, pp. 99–102, 2019.

[171] K. Antevski and C. J. Bernardos, "Federation of 5G services using distributed ledger technologies," *Internet Technology Letters*, p. e193, 2016.

[172] W. Lin, X. Xu, L. Qi, X. Zhang, W. Dou, and M. R. Khosravi, "A proof-of-majority consensus protocol for blockchain-enabled collaboration infrastructure of 5g network slice

brokers," in *Proceedings of the 2nd ACM International Symposium on Blockchain and Secure Critical Infrastructure*, 2020, pp. 41–52.

[173] A. Theodouli, S. Arakliotis, K. Moschou, K. Votis, and D. Tzovaras, "On the Design of a Blockchain-based System to Facilitate Healthcare Data Sharing," in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. IEEE, 2018, pp. 1374–1379.

[174] M. Ghadamyari and S. Samet, "Privacy-Preserving Statistical Analysis of Health Data Using Paillier Homomorphic Encryption and Permissioned Blockchain," in *2019 IEEE International Conference on Big Data (Big Data)*, 2019, pp. 5474–5479.

[175] K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, "Medblock: Efficient and Secure Medical Data Sharing via Blockchain," *Journal of medical systems*, vol. 42, no. 8, pp. 1–11, 2018.

[176] K. Ito, K. Tago, and Q. Jin, "i-Blockchain: a blockchain-empowered individual-centric framework for privacy-preserved use of personal health data," in *2018 9th International Conference on Information Technology in Medicine and Education (ITME)*. IEEE, 2018, pp. 829–833.

[177] A. Ekblaw, A. Azaria, J. D. Halamka, and A. Lippman, "A Case Study for Blockchain in Healthcare:"MedRec" Prototype for Electronic Health Records and Medical Research Data," in *Proceedings of IEEE open & big data conference*, vol. 13, 2016, p. 13.

[178] B. K. Mohanta, D. Jena, S. S. Panda, and S. Sobhanayak, "Blockchain Technology: A Survey on Applications and Security Privacy Challenges," *Internet of Things*, vol. 8, p. 100107, 2019.

[179] T. Kumar, V. Ramani, I. Ahmad, A. Braeken, E. Harjula, and M. Ylianttila, "Blockchain Utilization in Healthcare: Key Requirements and Challenges," in *2018 IEEE 20th International conference on e-health networking, applications and services (Healthcom)*. IEEE, 2018, pp. 1–7.

[180] J. Huang, L. Kong, G. Chen, L. Cheng, K. Wu, and X. Liu, "B-IoT: Blockchain driven Internet of Things with credit-based consensus mechanism," in *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2019, pp. 1348–1357.

[181] C. Huang, Z. Wang, H. Chen, Q. Hu, Q. Zhang, W. Wang, and X. Guan, "Repchain: A Reputation-based ecure, fast, and high incentive Blockchain System via Sharding," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4291–4304, 2020.

[182] S. Huh, S. Cho, and S. Kim, "Managing IoT Devices using Blockchain Platform," in *2017 19th international conference on advanced communication technology (ICACT)*. IEEE, 2017, pp. 464–467.

[183] D. Pavithran and K. Shaalan, "Towards Creating Public Key Authentication for IoT Blockchain," in *2019 Sixth HCT Information Technology Trends (ITT)*. IEEE, 2019, pp. 110–114.

[184] W. Ford and Y. Poeluev, "An efficient certificate format for ecc," 2015.

[185] N. Afraz and M. Ruffini, "A sharing platform for multi-tenant pons," *Journal of Lightwave Technology*, vol. 36, no. 23, pp. 5413–5423, 2018.

[186] X. Wang and Z. Zhang, "Data Division Scheme based on Homomorphic Encryption in WSNs for Health Care," *Journal of medical systems*, vol. 39, no. 12, p. 188, 2015.

[187] W. Guo, J. Shao, R. Lu, Y. Liu, and A. A. Ghorbani, "A privacy-preserving online medical prediagnosis scheme for cloud environment," *IEEE Access*, vol. 6, pp. 48 946–48 957, 2018.

[188] J. Sun, Y. Liu, and J. S. Dong, "Model checking csp revisited: Introducing a process analysis toolkit," in *International symposium on leveraging applications of formal methods, verification and validation*. Springer, 2008, pp. 307–322.

[189] P. Zhang, Y. Wu, and H. Zhu, "Open ecosystem for future industrial internet of things (iiot): architecture and application," *CSEE Journal of Power and Energy Systems*, vol. 6, no. 1, pp. 1–11, 2020.

[190] J.-S. Fu, Y. Liu, H.-C. Chao, B. K. Bhargava, and Z.-J. Zhang, "Secure data storage and searching for industrial iot by integrating fog computing and cloud computing," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 10, pp. 4519–4528, 2018.

[191] I. Cervesato, "The dolev-yao intruder is the most powerful attacker," in *16th Annual Symposium on Logic in Computer Science—LICS*, vol. 1. Citeseer, 2001, pp. 1–2.

[192] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *Ieee Access*, vol. 4, pp. 2292–2303, 2016.

[193] L. Guo and J. Qiu, "Combination of cloud manufacturing and 3d printing: research progress and prospect," *The International Journal of Advanced Manufacturing Technology*, vol. 96, pp. 1929–1942, 2018.

[194] M. Yampolskiy, J. Gatlin, and M. Yung, "Myths and Misconceptions in Additive Manufacturing Security: Deficiencies of the CIA Triad," in *Proceedings of the 2021 Workshop on Additive Manufacturing (3D Printing) Security*, 2021, pp. 3–9.

[195] Z. Bakhshi, A. Balador, and J. Mustafa, "Industrial iot security threats and concerns by considering cisco and microsoft iot reference models," in *2018 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*. IEEE, 2018, pp. 173–178.

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

[197] M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang, L. Shu *et al.*, "Authentication protocols for internet of things: a comprehensive survey," *Security and Communication Networks*, vol. 2017, 2017.

[198] J. Koch, K. Eggers, J.-E. Rath, and T. Schüppstuhl, "Development process for information security concepts in iiot-based manufacturing," in *International Conference on Flexible Automation and Intelligent Manufacturing*. Springer, 2022, pp. 316–331.

[199] A. Hassanzadeh, S. Modi, and S. Mulchandani, "Towards effective security control assignment in the industrial internet of things," in *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*. IEEE, 2015, pp. 795–800.

[200] I. Cvitić, M. Vujić *et al.*, "Classification of security risks in the iot environment." *Annals of DAAAM & Proceedings*, vol. 26, no. 1, 2015.

[201] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, "A survey of intrusion detection in internet of things," *Journal of Network and Computer Applications*, vol. 84, pp. 25–37, 2017.

[202] Z. A. Khan and P. Herrmann, "A trust based distributed intrusion detection mechanism for internet of things," in *2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA)*. IEEE, 2017, pp. 1169–1176.

[203] M. Cebe and K. Akkaya, "Efficient certificate revocation management schemes for iot-based advanced metering infrastructures in smart cities," *Ad hoc networks*, vol. 92, p. 101801, 2019.

[204] R. Latha and R. Bommi, "An analysis of intrusion detection systems in iiot," in *2023 Eighth International Conference on Science Technology Engineering and Mathematics (ICONSTEM)*. IEEE, 2023, pp. 1–10.

[205] C. Adaros Boye, P. Kearney, and M. Josephs, "Cyber-risks in the industrial internet of things (iiot): Towards a method for continuous assessment," in *Information Security: 21st International Conference, ISC 2018, Guildford, UK, September 9–12, 2018, Proceedings 21*. Springer, 2018, pp. 502–519.

[206] J. Höglund, S. Lindemer, M. Furuhed, and S. Raza, "Pki4iot: Towards public key infrastructure for the internet of things," *Computers & Security*, vol. 89, p. 101658, 2020.

[207] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Low-latency federated learning and blockchain for edge association in digital twin empowered 6g networks," *IEEE Transactions on Industrial Informatics*, 2020.

[208] K. Kaur, S. Guo, M. Chen, and D. Rawat, "Transfer learning for 5g-aided industrial internet of things," *IEEE Transactions on Industrial Informatics*, 2021.

[209] N. Kumar, S. Aggarwal, and P. Raj, *The Blockchain Technology for Secure and Smart Applications across Industry Verticals*. Academic Press, 2021.

[210] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for 5G and beyond networks: A state of the art survey," *Journal of Network and Computer Applications*, p. 102693, 2020.

[211] C.-Y. Lee, K. M. Kavi, R. A. Paul, and M. Gomathisankaran, "Ontology of secure service level agreement," in *2015 IEEE 16th International Symposium on High Assurance Systems Engineering*. IEEE, 2015.

[212] H. N. Qureshi, M. Manalastas, A. Imran, and M. O. Al Kalaa, "Service level agreements for 5g-enabled healthcare systems: Challenges and considerations," *IEEE network*, vol. 36, no. 1, pp. 181–188, 2021.

[213] J. Ortiz, R. Sanchez-Iborra, J. B. Bernabe, A. Skarmeta, C. Benzaid, T. Taleb, P. Alemany, R. Muñoz, R. Vilalta, C. Gaber *et al.*, "Inspire-5gplus: Intelligent security and pervasive trust for 5g and beyond networks," in *Proceedings of the 15th International Conference on Availability, Reliability and Security*, 2020, pp. 1–10.

[214] S. Sicari, A. Rizzardi, and A. Coen-Porisini, "5g in the internet of things era: An overview on security and privacy challenges," *Computer Networks*, vol. 179, p. 107345, 2020.

[215] A. Vance, "Flow based analysis of advanced persistent threats detecting targeted attacks in cloud computing," in *2014 First International Scientific-Practical Conference Problems of Infocommunications Science and Technology*. IEEE, 2014, pp. 173–176.

[216] W. A. Jansen, "Cloud hooks: Security and privacy issues in cloud computing," in *2011 44th Hawaii International Conference on System Sciences*. IEEE, 2011, pp. 1–10.

[217] Z. Yu, Q. Wang, W. Zhang, and H. Dai, "A Cloud Certificate Authority Architecture for Virtual Machines with Trusted Platform Module," in *2015 IEEE 17th International Conference on High Performance Computing and Communications*. IEEE, 2015, pp. 1377–1380.

[218] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta, and B. Ford, "Omniledger: A Secure, Scale-out, Decentralized Ledger via Sharding," in *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2018, pp. 583–598.

[219] A. Kiayias and G. Panagiotakos, "Speed-security Tradeoffs in Blockchain Protocols," *Cryptology ePrint Archive*, 2015.

[220] T. M. Hewa, Y. Hu, M. Liyanage, S. S. Kanhare, and M. Ylianttila, "Survey on blockchain-based smart contracts: Technical aspects and future research," *IEEE Access*, vol. 9, pp. 87 643–87 662, 2021.

[221] T. Hewa, A. Bracken, M. Ylianttila, and M. Liyanage, "Blockchain-based automated certificate revocation for 5g iot," in *ICC 2020-2020 IEEE International Conference on Communications (ICC)*. IEEE, 2020, pp. 1–7.

[222] T. Hewa, G. Gür, A. Kalla, M. Ylianttila, A. Bracken, and M. Liyanage, "The role of blockchain in 6g: Challenges, opportunities and research directions," *2020 2nd 6G Wireless Summit (6G SUMMIT)*, pp. 1–5, 2020.

[223] T. Hewa, A. Braeken, M. Ylianttila, and M. Liyanage, “Multi-access edge computing and blockchain-based secure telehealth system connected with 5g and iot,” in *GLOBECOM 2020-2020 IEEE Global Communications Conference*. IEEE, 2020, pp. 1–6.

[224] C. J. F. Cremers *et al.*, *Scyther: Semantics and verification of security protocols*. Eindhoven university of Technology Eindhoven, Netherlands, 2006.

[225] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuéllar, P. H. Drielsma, P.-C. Héam, O. Kouchnarenko, J. Mantovani *et al.*, “The avispa tool for the automated validation of internet security protocols and applications,” in *Computer Aided Verification: 17th International Conference, CAV 2005, Edinburgh, Scotland, UK, July 6-10, 2005. Proceedings 17*. Springer, 2005, pp. 281–285.

[226] S. Sayeed and H. Marco-Gisbert, “Assessing blockchain consensus and security mechanisms against the 51% attack,” *Applied sciences*, vol. 9, no. 9, p. 1788, 2019.

[227] J.-P. Aumasson, “The impact of quantum computing on cryptography,” *Computer Fraud & Security*, vol. 2017, no. 6, pp. 8–11, 2017.

[228] United Nations, “Transforming our world: The 2030 agenda for sustainable development,” 2015, accessed on 23.05.2023. [Online]. Available: https://sustainabledevelopment.un.org/post2015/transformingourworld

Original publications

I Hewa T, Braeken A, Ylianttila M & Liyanage M "Blockchain-Based Automated Certificate Revocation for 5G IoT." ICC 2020 - 2020 IEEE International Conference on Communications (ICC), IEEE, 2020, pp. 1–7. DOI.org (Crossref), https://doi.org/10.1109/ICC40277.2020.9148820.

II Hewa T, Braeken A, Liyanage M & Ylianttila M. "Fog Computing and Blockchain-Based Security Service Architecture for 5G Industrial IoT-Enabled Cloud Manufacturing." IEEE Transactions on Industrial Informatics, vol. 18, no. 10, Oct. 2022, pp. 7174–85. DOI.org (Crossref), https://doi.org/10.1109/TII.2022.3140792.

III Hewa T, Kalla A, Porambage P, Liyanage M & Ylianttila M "How DoS Attacks Can Be Mounted on Network Slice Broker and Can They Be Mitigated Using Blockchain?" 2021 IEEE 32nd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), IEEE, 2021, pp. 1525–31. DOI.org (Crossref), https://doi.org/10.1109/PIMRC50174.2021.9569375.

IV Hewa T, Porambage P, Kovacevic I, Weerasinghe N, Harjula E,Liyanage M & Ylianttila M. "Blockchain-Based Network Slice Broker to Facilitate Factory-As-a-Service." IEEE Transactions on Industrial Informatics, vol. 19, no. 1, Jan. 2023, pp. 519–30. DOI.org (Crossref), https://doi.org/10.1109/TII.2022.3173928.

V Hewa T, Porambage P, Kalla A, Pamela D, Liyanage M & Ylianttila M. "Blockchain and Game Theory Convergence for Network Slice Brokering." Computer, vol. 56, no. 3, Mar. 2023, pp. 80–91. DOI.org (Crossref), https://doi.org/10.1109/MC.2022.3165533.

VI Hewa T, Porambage P, Liyanage M & Ylianttila M. "Bulletproofs based Novel Privacy-preserved Consensus Protocol for 5G connected IoT Data" Journal article submitted to IEEE Transactions on Network and Service Management.

Reprinted with permission from IEEE (I), IEEE(II), IEEE (III), IEEE(IV), IEEE (V)

Original publications are not included in the electronic version of the dissertation.

ACTA UNIVERSITATIS OULUENSIS

SERIES C TECHNICA

898. Baubekova, Aziza (2023) Catchment-estuary-coastal systems under climate change and anthropogenic pressure

899. Akbari, Mahdi (2023) Application of remote-sensing and machine-learning in studying the climatic and anthropogenic drivers of water bodies drying in data-scarce transboundary basins

900. Kaikkonen, Pentti (2023) Characteristics of ultrafine/nanostructured bainite formation in low-temperature ausformed medium-carbon steels

901. Su, Zhuo (2023) LBP inspired efficient deep convolutional neural networks for visual representation learning

902. Cui, Yawen (2023) Few-shot learning for image classification

903. Bhayani, Snehal (2023) Sparse resultant-based methods with their applications to generalized cameras

904. Mehmood, Hassan (2023) Concept drift in smart city scenarios

905. Talala, Tuomo (2023) A CMOS SPAD line sensor and timing skew compensation techniques for time-resolved Raman spectroscopy

906. Nasim, Sofeem (2023) Low cost sensory modeling approach for environmental monitoring and sustainability

907. Jalali Shahrood, Abolfazl (2023) Past, present, and future of river flow regime in Nordic region focusing on river ice break-up events

908. Inkeröinen, Jouko (2023) Towards complexity competence in environmental research governance

909. Nguyen, Hong Tri (2023) A transition towards decentralized service market : blockchain-based enablers, challenges, and solutions

910. Hamdard, Mohammad Hamid (2023) An assessment of drinking water quality in Afghanistan

911. Matinheikki, Matti (2023) Lopputuotevaatimuksiin perustuva hankinta-, toteutus- ja arviointimalli kaupunkialueiden kunnossapidon alueurakoissa : tilaajan ja asiakkaan aktiivinen rooli projektin aikana

912. Noor, Kashif (2023) Spatiotemporal evaluation of snowmelt water and snowpack isotopes (^{18}O and ^{2}H) and their application in subarctic catchment hydrology

913. Hietala, Sanna (2023) Environmental life cycle assessment of livestock production : the applicability of IPCC and PEFCR methods to Finnish production

Book orders:
Virtual book store
https://verkkokauppa.omapumu.com/fi/

UNIVERSITY OF OULU P.O. Box 8000 FI-90014 UNIVERSITY OF OULU FINLAND

ACTA UNIVERSITATIS OULUENSIS

UNIVERSITY OF OULU

ISBN 978-952-62-3913-2 (Paperback)
ISBN 978-952-62-3914-9 (PDF)
ISSN 0355-3213 (Print)
ISSN 1796-2226 (Online)