Received January 4, 2021, accepted January 9, 2021, date of publication January 14, 2021, date of current version January 26, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3051602

Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network

SAURABH SINGH[1], A. S. M. SANWAR HOSEN[2], AND BYUNGUN YOON[1], (Senior Member, IEEE)

[1]Department of Industrial and Systems Engineering, Dongguk University, Seoul 04620, South Korea
[2]Division of Computer Science, Jeonbuk National University, Jeonju 54896, South Korea

Corresponding author: Byungun Yoon (postman3@dongguk.edu)

This work was supported in part by the National Research Foundation of Korea under Grant 2019R1A2C1085388, and in part by the Dongguk University Research Fund of 2020 under Grant S-2020-G0001-00050.

ABSTRACT Blockchain technology is becoming increasingly attractive to the next generation, as it is uniquely suited to the information era. Blockchain technology can also be applied to the Internet of Things (IoT). The advancement of IoT technology in various domains has led to substantial progress in distributed systems. Blockchain concept requires a decentralized data management system for storing and sharing the data and transactions in the network. This paper discusses the blockchain concept and relevant factors that provide a detailed analysis of potential security attacks and presents existing solutions that can be deployed as countermeasures to such attacks. This paper also includes blockchain security enhancement solutions by summarizing key points that can be exploited to develop various blockchain systems and security tools that counter security vulnerabilities. Finally, the paper discusses open issues relating to and future research directions of blockchain-IoT systems.

INDEX TERMS Blockchain, Internet of Things, threats and attacks, security.

I. INTRODUCTION

Blockchain technology, a distributed digital ledger technology that can be used to maintain continuously growing lists of data records and transactions securely, has recently taken the world by storm. The three main criteria related to blockchain identity and accessibility are public or less authorized, private or authorized, and consortium. The most important and unique factor of the blockchain concept is that the stored information is secured entirely within the blocks of the blockchain's transactions. Its decentralized consensus model has the three main features of consistency, aliveness, and fault tolerance [1]–[3].

Blockchain technology has been successfully applied in a wide variety of areas. When blockchain technology is implemented in the Internet of Things (IoT) domain to exchange and share network data, records, validation, and security service, there are a few relevant issues that are still being researched, with a particular focus on the security of cyber-physical systems in the IoT sector. Many authorized organizations are currently working to ensure proper interoperability, integrity, and privacy of the IoT network. These organizations are all working together using blockchain technology and cloud computing. The technology brings transparency, reliability, and proper governance to the IoT information system [4]–[7].

Blockchain technology is redefining data modeling, and governments have implemented blockchain in many IoT applications. It is mainly attractive for such applications due to its unprecedented ability to adapt as well as the segment, protect, and share IoT data and services. Blockchain technology is at the center of many current developments in the IoT industry. One reason for this is that many IoT services are vulnerable to attacks and challenges. Using blockchain technology can solve many of the issues with cyber-physical systems in the IoT sector. As the IoT industry is moving toward a network sensor model, sustainable smart cities, and the many components involved must be framed in consideration of certain benefits [8]–[12].

Moreover, blockchain enables different privacy-preserving models for IoT applications, such as data privacy, user privacy, location privacy, privacy-preserving aggregation, and

The associate editor coordinating the review of this manuscript and approving it for publication was Chunhua Su.

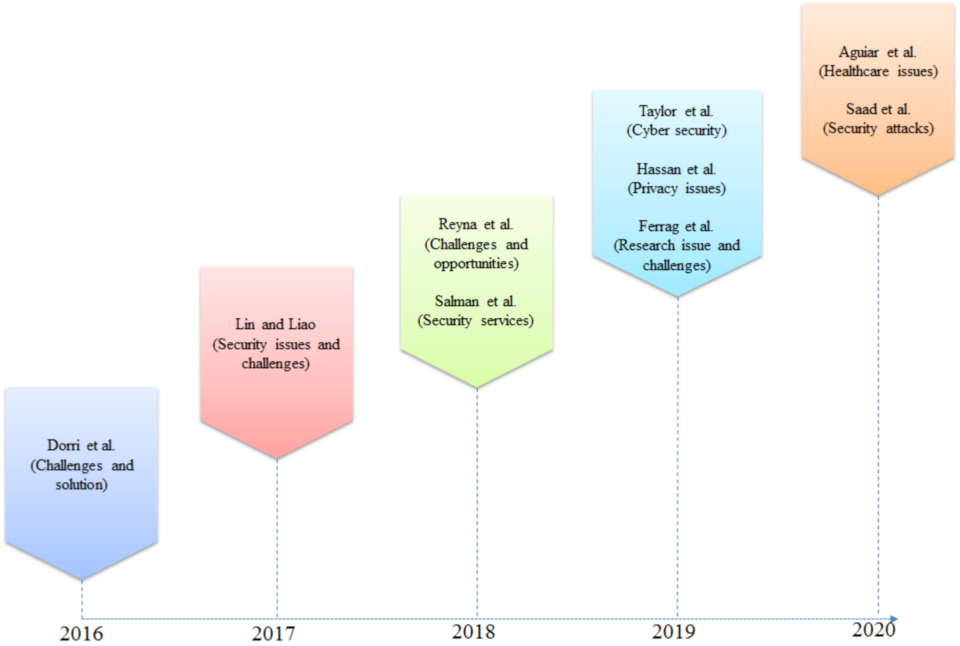


FIGURE 1. **Roadmap of different literature on security issues, attacks, and solutions in blockchain technology between 2016 and 2020.**

many others. Ferrag *et al.* [13] suggested many privacy-preserving schemes and presented a side-by-side comparison of different security and privacy approaches for Fog-based IoT applications. Dwivedi *et al.* [14] proposed a scheme of modified blockchain models in the medical sector that involves additional protection and privacy parameters based on advanced cryptographic primitives. This scheme uses lightweight digital signatures to guarantee that the information cannot be improperly modified, and a tamper-proof seal protects it. Privacy-preserving methods for IoT data in smart cities have been discussed by Shen *et al.* [15]. Support vector machine training is used with blockchain technology to enable it to handle smart city data. The blockchain techniques allow for secure and reliable IoT data between data providers, where each provider can encrypt the data instance locally using its private key.

In the move toward numerous beneficial features such as decentralization, persistence, anonymity, and auditability, security is a major concern. This paper provides an inclusive overview of blockchain parameters and security attacks in cyber-physical systems. It also presents some existing solutions and blockchain applications for various factors that can affect the blockchain system. Blockchain technology has attracted substantial industrial and academic attention due to its decentralization, persistence, anonymity, and auditing attributes. In this survey, we consider the implementation of blockchain technology in a wide range of applications and discuss a number of the challenges involved.

A. CONTRIBUTION

1) To the best of our knowledge, this is the first study of its kind to survey blockchain attacks in IoT networks and provide solutions for such attacks.
2) This review presents the essential background knowledge needed for blockchain and its elements, participants, and components along with their functionalities. The goal is to familiarize readers with the blockchain system. Moreover, this paper systematically presents and discusses the security limitations, vulnerabilities, challenges, and issues associated with blockchain technology, as well as security issues in blockchain enterprises.
3) This paper discusses the widespread security attacks on blockchain technologies and their vulnerabilities based on the results of many existing studies. Moreover, various applications and opportunities involved in blockchain technology are also discussed.
4) This survey presents existing security solutions for blockchain technology in different environments. Finally, this paper discusses some security tools that can address these security vulnerabilities. It also outlines some open questions and research challenges, and open requirements that could improve blockchain-IoT capability.

B. ROADMAP AND COMPARISON WITH RELATED SURVEY ARTICLE

Fig. 1 shows a roadmap of the various kinds of surveys related to blockchain technology presented from 2016 to 2020. Dorri *et al.* considered IoT security and privacy issues and vulnerabilities [S1]. The authors also provided a blockchain-based solution. Lin and Liao [S2] surveyed the blockchain security issues and challenges as well as the different kinds of attacks. They also briefly discussed other blockchain applications such as Bitcoin, Ethereum, and hyper ledger.

Reyna *et al.* surveyed blockchain technology with a focus on feature analysis and challenges, as well as the integration of blockchain and IoT through different identification and analysis methods. Applications based on blockchain-IoT are also discussed. However, there is limited research on security attacks, although a solution has been proposed by Reyna *et al.* [S3]. Salman *et al.* [S4] illustrated blockchain-based approaches for several security services, including resource provenance, confidentiality, authentication, integrity assurance, and privacy.

They also discussed some of the challenges and issues associated with blockchain-based security services, and provided insight into security services in current applications and techniques. Taylor *et al.* [S5] provided a systematic literature survey on blockchain cybersecurity, including research-type applications, and reported key qualitative/quantitative data. They also discussed future research directions in blockchain for IoT security, artificial intelligence (AI) data security, and the release of open-source software and datasets. Hassan *et al.* [S6] discussed privacy-preserving features in blockchain-based IoT systems. The authors focused on presenting the practical issues caused by privacy leakages in IoT operating systems, analyzing the implementation of privacy protection, and outlining the various issues associated with the privacy protection of blockchain-based IoT systems. Ferrag *et al.* [S7] discussed different application domains of blockchain–IoT, such as IoV, IoE, IoC, edge computing, and others. They reviewed the anonymity and privacy of the bitcoin system and provided a taxonomy with a side-by-side comparison of state-of-the-art privacy-preserving blockchain technology. Aguiar *et al.* [S8] surveyed blockchain-based strategies for healthcare applications. They analyzed the tools employed by industries in that area to construct blockchain networks. The paper also discussed privacy techniques and access control employed in healthcare records using case scenarios for monitoring patients in remote care environments. Saad *et al.* [S9] systematically explored the attack surface in terms of blockchain cryptographic construct, distributed architecture, and blockchain application context, while providing detailed solutions and opportunities.

This paper is organized as follows: Section II explains blockchain technology and its related factors. Section III provides details about blockchain security attacks, and section IV discusses the blockchain security issues. Section V discusses blockchain challenges, and Section VI surveys the different blockchain technology solutions for the challenges in various sectors. Section VII discusses open issues and potential future research directions. Finally, Section VIII concludes the paper.

II. BLOCKCHAIN FACTORS and ISSUES

This section discusses the key factors and issues related to blockchain implementation in smart networks, including existing solutions and recommendations.

A. ELEMENTS IN BLOCKCHAIN AND RELATED CONCERNS

1) DECENTRALIZATION

In blockchain technology, decentralization entails dispersing functions throughout a system rather than having all units connected with and controlled by a central authority; in other words, there is no central point of control, and this absence of centralized authority in a blockchain is what makes it more secure than other technologies. Each blockchain user, called a miner, is assigned a unique transaction account, and blocks are added once the miners are validated. The decentralized nature of the data records used in blockchain technology exemplifies its revolutionary quality; blockchain networks use consensus protocols to secure nodes. In this way, transactions are validated and data cannot be destroyed. While the decentralized nature of networks allows for peer-to-peer operations [16], it also poses major challenges to personal data privacy [17]. Gai *et al.* [18] surveyed some of these security and privacy issues, which include threats, malicious adversaries, and attacks in financial industries. Zyskind *et al.* [19] examined decentralized personal data management in the context of personal data privacy concerns.

2) CONSENSUS MODEL

Consensus refers to agreement among entities [20], and consensus models help decentralized networks make unanimous decisions. This allows for all records to be tracked from a single authority. Blockchain technology requires consensus algorithms to ensure that each next block is the only true version; that is, the algorithms ensure that all nodes agree that each new block added to the blockchain carries the same message. Consensus models guarantee against ‘‘fork attacks’’ and can even protect against malicious attacks [21]. The three main features of consensus models are as follows:

1) *Consistency*- this protocol is safe and consistent when all nodes produce the same output.
2) *Aliveness*- the consensus protocol guarantees aliveness if all participating nodes have produced a result.
3) *Fault tolerance*- the mechanism delivers fault tolerance for recovery from failure nodes.

3) TRANSPARENCY AND PRIVACY

The most appealing aspect of blockchain technology is the degree of privacy it offers, but this can create some confusion regarding transparency. Blockchain networks periodically (i.e., every 10 minutes) self-audit the digital value ecosystems that coordinate transactions; one set of these transactions is called a block, and this process results in two properties: transparency and impossibility of corruption. In a blockchain, the identity of the user is hidden behind a strong cipher, making it particularly difficult to link public addresses to individual users. The question thus arises of how blockchain can be regarded as truly transparent [22].

Blockchain is already regarded as a powerful technology [23]. It organizes interactions in such a way that greatly

TABLE 1. Comparison of related surveys.

Article	Year	Focused on	Security Attacks	Classification	Opportunities	Applications	Solutions	Security tools
[S1]	2016	Proposing a secure, private, and lightweight architecture for IoT based on blockchain technology	Yes	No	No	No	Yes	No
[S2]	2017	Introducing preliminaries of blockchain and security issues in blockchain	No	No	No	Yes	No	No
[S3]	2018	Investigating the challenges in IoT applications integrated with blockchain.	Yes	No	Yes	Yes	No	No
[S4]	2019	Blockchain-based solutions for security issues.	No	No	No	No	Yes	No
[S5]	2019	Blockchain applications in cybersecurity	No	No	No	Yes	No	No
[S6]	2019	Privacy issues caused by the integration of IoT with blockchain	Yes	Yes	No	No	No	No
[S7]	2019	Surveying existing blockchain protocols used with IoT	Yes	Yes	No	Yes	Yes	No
[S8]	2020	Applications of blockchain in the healthcare domain	No	No	No	No	Yes	No
[S9]	2020	Exploring the attack surface of the public blockchain	No	Yes	No	Yes	Yes	No
This Survey	2020	All of the above	Yes	Yes	Yes	Yes	Yes	Yes

improves reliability while also eliminating the business and political risks associated with managing processes through central entities, thus reducing the need for trust. Blockchain networks create platforms that can simultaneously run different applications from different companies, enabling seamless and efficient dialogue and the creation of audit trails through which everyone can verify that everything is being processed correctly.

4) IDENTITY AND ACCESS

Blockchain is a secure distributed ledger technology (DLT) that has taken on a new role in recent years. Jacobovitz *et al.* [24] discussed the state of the art in blockchain technology, applications, and solutions regarding identity management. Taking identity and access control to the next level and investigating whether the use of blockchain technology improves the management of device ID comprises one of the priority security projects of Sentara Healthcare, and Virginia and North Carolina are connected via an integrated distribution system [25]. According to industry expert Jeremy Kirk, there are currently six ongoing projects addressing how blockchain could make it easier to manage identity: Hyperledger Independent, Civic, Sovran, Evernym, Alastria, and uPort.

The three main criteria related to blockchain identity and accessibility are public or less authorized, private or authorized, and consortium. Pilkington [26] presented the main distinction between public and private blockchain technologies and discussed the foundations and disruptive nature of blockchain technology. Public blockchains are completely open and allow anyone to join the network; they are designed to reduce intermediaries so that more participants can join. By contrast, private blockchains restrict network privileges; participants need permission to join and the access control mechanism can change.

5) OPEN SOURCE

With distributed and closed-source applications, users must trust the applications, and they cannot access any data from central sources. It is possible to launch decentralized closed-source applications and achieve desired results, but doing so would have catastrophic consequences. This is a major reason that participants prefer decentralized open-source applications, with relevant platforms including Ethereum, Bitcoin cash, Litecoin, and Dash. Sidechain-capable blockchain platforms provide powerful benefits developed by community members such as

1) flexible configurations: no risk in multi-block reorganization and enables rapid transactions,
2) confidential transactions: leveraging stability,
3) federated two-way peg: issuing multi-transferrable assets on single blockchains, and
4) multiple assets issuance: secured by a federation of parties with aligned incentives.

Open-source applications help users adopt new technologies. One of the main features of such applications, as emphasized by Buterin [23], is an open-source license model and government mechanism that enables changes in public ledger currency platforms or blockchain applications. Tech giant IBM has helped evolve open-source technologies by promoting projects such as Linux Foundation's Hyperledger Composer; regarding enterprise ecosystems, MentaGo provides a blockchain solution for financial systems and SXSW uses Hyperledger fabric and IBM [27], [28].

6) ANONYMIZATION

Anonymity is one of the most important elements (shown in Fig. 2) in blockchain technology for maintaining the privacy of transactions in networks, but ensuring anonymity is difficult because the blockchain ledger is public. Each user generates an address, and there is no mechanism for

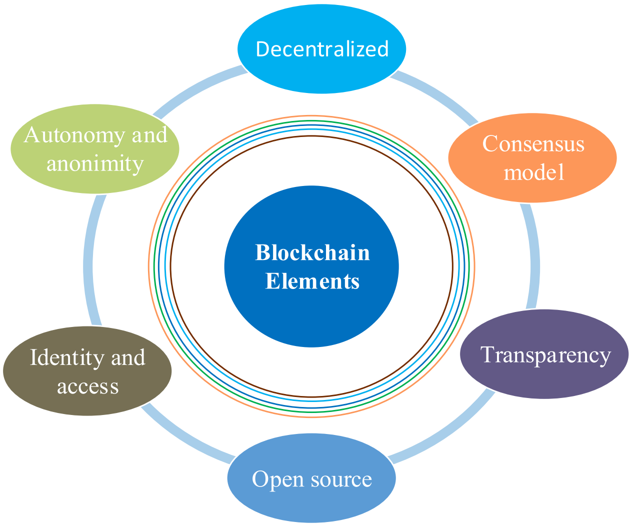


FIGURE 2. **Blockchain elements.**

keeping user information private. This is why Bitcoin is considered pseudo-anonymous: users can be linked with their public addresses, but it is not possible to learn their actual names or addresses [29]. Möser [30] presented an article on the anonymity of Bitcoin transactions in which a special Bitcoin mixing service was proposed that could complicate or confuse originating Bitcoin transaction addresses and thereby increase anonymity. The main security concern with blockchain is that public keys and transactions must not reveal real identities.

B. BLOCKCHAIN PARTICIPANTS AND RELATED CONCERN

Blockchain networks allow participants to reach consensus, and they also store data that can be accessed by all participants. Here, we discuss the different roles of blockchain network participants.

1) BLOCKCHAIN USERS

Users operate in blockchain networks, and their numbers have increased exponentially since 2011, according to Blockchain.info. This statistical portal also reported that the number of blockchain users was expected to reach 50 million by the end of 2020 [31]. There is a privacy issue facing blockchain users in the network.

2) BLOCKCHAIN REGULATOR

Achieving overall authority in business networks may require broad access to ledger contents. Kakavand *et al.* [32] presented an in-depth analysis of the current regulatory landscape of distribution technology, and Yeoh [33] discussed the regulatory issues involved with blockchain technology. He addressed the key regulatory challenges associated with innovative distributed blockchain technology across Europe and the United States.

3) BLOCKCHAIN DEVELOPER

Developers design both the applications and the smart contracts used by blockchain users. There are significant market opportunities for developers to cryptographically ensure the accuracies of the ledgers at the hearts of cryptocurrencies. Nordrum [34] presented a time frame for blockchain developers and described that developers have limited software tools with which to build secure blockchain ledgers.

4) CERTIFICATE AUTHORITY

This manages the heterogeneous certificates needed to run a permissioned blockchain using a trusted third party; Bitcoin and Ethereum are examples of permissioned blockchains. The authority authorizes the limited set of legitimate readers or writers [35]. The main issue in blockchain networks is trust. To address the issue of trust, blockchains distribute ledgers among many servers under different control authorities, but there is still a bootstrap problem associated with finding initial ledgers [36].

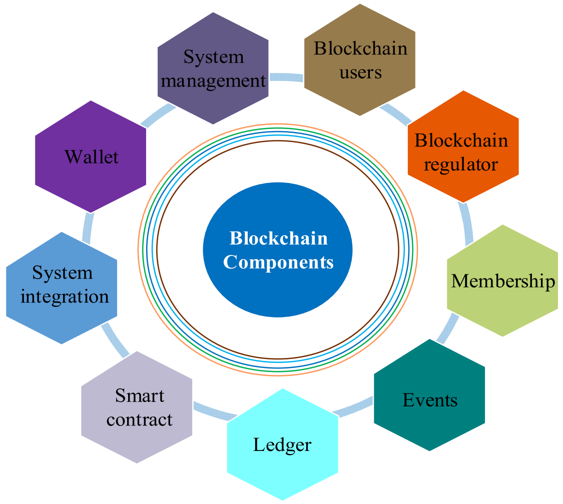


FIGURE 3. **Blockchain components.**

C. BLOCKCHAIN COMPONENTS

Fig. 3 shows many of the essential components of a blockchain. Detailed descriptions of each component are as follows:

Ledger: Contains the current world state of the blockchain transactions.

Smart Contract: Encapsulates the business network transactions into code. A transaction call causes the ledger state to be retrieved and set.

Consensus network: A set of data and processing peers that continually maintain the replicated ledger.

Membership: Manages identity and transactional certificates and other aspects of access rights.

Events: Generates notifications about important actions in the blockchain (such as new blocks) as well as notifications related to smart contracts with no event distribution.

System management: Provides the ability to create, change, and monitor blockchain components.

Wallet: Securely manages security credentials.

System Integration: Is responsible for integrating blockchains in a bidirectional manner with external systems.

D. SUMMARY AND INSIGHTS

Section II has discussed the security concerns and benefits of blockchain elements, such as decentralization, which pose major challenges for data privacy and transparency and lead to confusion in the network. In addition, the open-source and anonymous nature provide flexible configuration, confidentiality, and privacy in transactions. We have also discussed the security concerns of blockchain participants and components.

III. ATTACKS

In this section, we present different blockchain network applications and attacks as well as future opportunities in various sectors. For this subsection, we surveyed real blockchain attacks that commonly occur. We also referred to Li *et al.* [37], who discussed blockchain attacks and security risks. Here, we discuss some of these attacks in further detail.

1) Liveness Attack: Kiayias and Panagiotakos [38] stated that these attacks can delay the acknowledgment times of target transactions, and presented two examples of such attacks against Bitcoin and Ethereum. The liveness attack proceeds in three stages: preparation, transaction denial, and blockchain delay [39]. This attack delays the transaction confirmation time. In the preparation phase, the attacker tries to gain a potential advantage against honest players to build their private chain. Next is the transaction denial phase, in which the attacker attempts to delay the genuine block that contains the transaction, and when the attacker decides the delay is unconvincing, they proceed to the blockchain render phase, where they try to decrease the rate at which the chain transaction grows.

2) Double Spending Attacks: This problem is generated when one successful transaction is duplicated with the same funds; it represents a potential flaw in digital cash, as the same digital token can be spent two times when such an attack occurs. It is impossible to avoid double-spending, even though the blockchain consensus mechanism validates all transactions [40]. The authors of a research study by the Bank of Canada said that ''if a miner controls more than half of computational capacity amongst all miners, in theory, loses their power to control double spending incentives. A malicious miner can do this or dishonest who creates a larger arrival rate than the sum of all other legitimate or honest miners'' [41], [42]. Attacks related to double spending include race, Finney, 51%, and Vector 76 attacks.

3) 51% Vulnerability Attack: Blockchains rely on distributed consensus mechanisms to establish mutual trust. However, there is a 51% vulnerability in the consensus mechanism that an attacker can exploit to control the entire blockchain. Specifically, in a PoW-based blockchain, if a single minor hash function occupies more than 50% of the entire blockchain's total hash function, a 51% attack may be initiated. Thus, if the mining power is concentrated in several mining pools, unexpected situations can arise, such as a case in which a single pool controls more than half of all computing power. For example, in one real case, the mining pool ''ghash.io'' accounted for more than 42% of the total bitcoin mining power. The fact that a single mining pool represented such a high proportion was a serious concern, and many miners dropped out of the pool [43]. By starting a 51% attack, an attacker can arbitrarily manipulate and change blockchain information and perform the following actions [44], [45]:

1) reverse the transaction and initiate a double-spending attack
2) exclude and specify transaction orders
3) obstruct the general mining operations of other miners
4) impede the verification of normal transactions

4) Private Key Security Attack: A private key allows individuals to access funds and verify transactions; it is only created once and cannot be recovered if lost. Malicious actors perform a variety of actions to steal cryptocurrency by targeting key custodial services because cryptographic keys are particularly attractive targets. An attacker who has discovered vulnerability in an elliptic curve digital signature algorithm can recover a user's private key, and if a private key is stolen, it is difficult to track any related criminal activity and recover the relevant blockchain information [45]–[49]. FireEye Threat Intelligence has detected several prominent crimeware families with this functionality: Dridex, Terdot, IceID, SmokeLoader, BlackRubyRansomware, and Corebot.

5) Transaction Privacy Leakage: Because user behavior in blockchains is traceable, a blockchain system must take some measures to protect users' transaction privacy. However, some leakage of confidential information such as cryptographic keys can still occur, leading to the potential for people to commit real-world crimes. For instance, Bitcoin and Zcash use a one-time account to store received cryptograms, and users must also assign a secret key to each transaction. In this way, an attacker cannot infer whether the same transaction has involved a password violation by another person. Moreover, an attacker cannot infer the actual coin's linkage consumed by the transaction because the user can include several chaffcoins (called ''mixins'') when starting the transaction [50].

Wallet privacy leakage can also occur, where common bitcoin wallet operations leak some user information [51]; this leakage has been exploited in the past. Paul Fremantle *et al.* [52] proposed an architecture for IoT security and privacy that resolves the leakage issue.

6) Selfish Mining Attack: Selfish mining attacks are committed by some miners to waste legitimate miners' computing power or obtain unearned rewards. Such attackers attempt to fork the private chain by making the discovered block private [53], then self-employed miners try to maintain a longer private branch than the public branch to dig through this private chain and personally hold more newly found blocks; during this time, honest miners continue to dig in the public chain [54]. As the public domain approaches the length of the private branch, the new block mined by the attacker is revealed, thus wasting honest miners' computing power and keeping them from earning what they should earn. As a result, the selfish miners gain a competitive advantage over real miners [55]. By further strengthening attackers' mining rights, these attacks undermine the intended decentralized nature of blockchain technology.

7) DAO Attack: Decentralized autonomous organizations (DAOs) have been used as venture capital funds for crypto and distributed spaces because the lack of centralized authority minimizes costs and provides investors with more control and access. The cost savings coding framework in the absence of central power was developed by the German startup Slock.it as an open-source platform for building smart locks, but it was fully deployed underneath and distributed to "The DAO,'' a member of the Ethereum community [56], [57].

Ethereum deployed DAO as a smart contract in 2016 on a crowdfunding platform. The DAO contract was assaulted after being deployed for 20 days. It had raised approximately US$120 million before the attack, and the attacker stole around $60 million, making it the largest attack on the Ethereum consensus model. In this case, the attacker exploited reentrant vulnerability. First, the attacker exposed a malicious smart contract with a callback function, including the DAO's withdrawal function call. Withdraw () sent Ether to the called party, and this also occurred in the form of a call. Therefore, the malicious smart contract's callback function was called again. In this way, an attacker was able to steal all the Ether from DAO. Smart contract vulnerabilities have been exploited in other cases as well [58].

8) BGP Hijacking Attack: The Border Gateway Protocol (BGP) is used to share routing information networks on the internet, which specify how IP packets are forwarded to their destinations. An attacker can intercept the blockchain network by manipulating the BGP, after which data can be routed and the traffic can be modified to the attacker's favor [56].

Apostolakiet al. [59] considered small- and large-level attacks targeting individual nodes or the whole network and their impacts on Bitcoin. Due to the increased concentrations of some of Bitcoin's mining pools, BGP hijacking represents a major vulnerability; an attacker can effectively divide the Bitcoin network and slow the block propagation speed. As stated by Dell SecureWorks in 2014, BGP hijacking intercepts connections to the Bitcoin mine's mine pool server [60].

9) Balance Attack: For a balance attack, an attacker simply introduces a delay between valid subgroups with the same mining power, then executes the transaction in one of these subgroups. Next, the attacker mines enough blocks in other subgroups to ensure that the subtree of the other subgroup is more important than the transaction subgroup. Even if a transaction is not committed, an attacker can create a block with such a transaction that has a high probability of exceeding the subtree that contains this transaction.

10) Sybil Attack: This attack destroys the reputation system in a computer security system by forging an identity in the peer-to-peer network. If nodes are required to prove their identities before joining the network, as is the case in permissioned or private blockchains, they will not be able to forge identities. Soska and Christin (2015) proposed the ''Beaver'' system, which protects users' privacy while resisting Sybil attacks by charging fees [61].

A. SUMMARY AND INSIGHTS

This section discusses different attacks on the blockchain network. We address the liveness attack, which delays the transaction confirmation time; double-spending attacks, which duplicate the transaction funds; 51% vulnerability attacks, where adversaries can exploit more than 50% in the consensus mechanism; and private Key security attacks, in which an attacker discovers a vulnerability in the elliptic curve digital signature used in encryption methods, privacy leakage, and self-mining. Other attacks are also explained in detail.

IV. BLOCKCHAIN SECURITY ISSUES

1) Transaction Malleability: During contracted transactions, the agreement does not immediately cover all the information in the hashed transaction; therefore, it is rare but possible for a node to change a transaction in the network in such a way that the hash is not validated. Christian Decker and Roger Wattenhofer defined transaction malleability as when transactions are intercepted, modified, and rebroadcast, thus leading the transaction legal entity to believe that the original transaction was not confirmed [62], [63].

2) Network Security: An eclipse attack occurs when an opponent controls pieces of network communication and logically divides the network to increase synchronization delay [61]; an example is a simple denial of service attack to improve selfish mining and double-spending [65], [66]. In eclipse attacks, an attacker selects and hides information from one or more participants, potentially by delaying the delivery of blocks to a node.

3) Privacy: Privacy and confidentiality are still major concerns with blockchain transactions because each node can access data from another node, and anyone viewing the blockchain can see all transactions [67]. Studies have suggested various ways to overcome this problem, but these methods are only practical for specific applications, and they do not cover all issues. Due to the enormous number of data transmissions, communications involving important data in the network might be attacked by some adversaries through attacks such as the man-in-the-middle (MitM) attack and the DoS/DDoS attack. IoT poses many unique privacy challenges, such as data privacy and tracking concerns for phones and cars. In addition, voice recognition is being integrated to allow devices to listen to conversations to actively transmit data to cloud storage for processing [68], [69].

4) Redundancy: Expensive duplication for the purpose of eliminating the arbitration that allows each node of the network to have a copy of every transaction. However, it is both financially and legally illogical to have redundant brokering; banks are not willing to perform every transaction with every

TABLE 2. Items available through criminal enterprises.

Category	Number of Items	Percentage (%)	Related Information and Title	Money Seized	Reference
Weed	3338	13.7	"From Seeds to Weed, Bitcoin Finds Home Where Commerce Goes Gray" (https://www.coindesk.com/bitcoin-atms-gray-areas)	$141.8 Billion	[74] [75]
Drugs	2194	9.0	"Blockchain in Action: Derailing Drug Abuse & Prescription Drug Fraud" (https://blockchain.wtf/2018/06/series/blockchain-in-action/derailing-drug-abuse/) "Tracing Illegal Activity Through the Bitcoin Blockchain To Combat Cryptocurrency" (https://www.forbes.com/sites/rachelwolfson/2018/11/26/tracing-illegal-activity-through-the-bitcoin-blockchain-to-combat-cryptocurrency-related-crimes/#18aa339b33a9)	$72 Billion	[76] [77]
Prescriptions	1784	7.3	"Bitcoin: Economics, Technology, and Governance" (https://pubs.aeaweb.org/doi/pdfplus/10.1257/jep.29.2.213) "Blockchain Aims to Curb Prescription Drug Abuse" (https://hackernoon.com/blockchain-aims-to-curb-prescription-drug-abuse-47fc9cc66379)		[76] [78] [79] [80]
Benzodiazepines	1193	4.9	A class of psychoactive drugs	$3.6 Million	[79]
Cannabis	877	3.6	"Blockchain for Crime Prevention in the Legal Cannabis Space" (https://investingnews.com/innspired/blockchain-crime-prevention-legal-cannabis-space/)		[80] [81]
Hash	820	3.4	"The Future of Blockchain technology and cryptocurrencies" (https://skemman.is/bitstream/1946/30832/1/The%20future%20of%20blockchain%20technology%20and%20cryptocurrencies.pdf) "The Dark Side of Bitcoin" (https://blog.blockonomics.co/the-dark-side-of-bitcoin-illegal-activities-fraud-and-bitcoin-360e83408a32)		[82] [84]
Cocaine	630	2.6	"How the Feds Took Down the Silk Road Drug Wonderland" (https://www.wired.com/2013/11/silk-road/) "Heroin, Cocaine and LSD Sales Transactions Were Stopped Using Digital Currency BitCoin"		[83]
Pills	473	1.9	"Drug Dealers Are Using Bit Coins to Fund the Flooding-Fatal Fentanyl Waves in Foreign Countries" "From the Dark Side of Bitcoin: Misusing Cryptography" (https://99bitcoins.com/the-dark-side-of-bitcoin-misusing-cryptography/)	$10 million	[80] [84]

bank or complete other banks' transactions. Such duplication only increases costs while providing no conceivable benefits [70].

5) Regulatory Compliance: Blockchains exist regardless of the law, and government authorities do not necessarily change how they do their jobs in response to the existence of blockchains. Applying blockchain technology in the legal and financial sectors in non-Bitcoin currencies creates regulatory challenges, but infrastructure regulation is very similar to blockchain regulation [70]. Yeoh [33] discussed the key regulatory issues affecting the blockchain and innovation distributed technology that has been adopted across Europe and the United States.

6) Criminal Activity: Bitcoin-enabled third-party trading platforms allow users to purchase or sell a wide variety of products. These processes are anonymous, making it difficult to track user behavior and impose legitimate sanctions. Criminal activity involving Bitcoin frequently involves ransomware, underground markets, and money laundering [71]. Some underground markets that operate online trade as Tor hidden services use Bitcoin exchange currency, thus making blockchain availability uncertain because of criminal activity. Table 2 lists the top 10 item available categories [72].

7) Vulnerabilities in Smart Contracts: When a program is executed in a blockchain, a smart contract can have security vulnerabilities caused by a flaw in that program. For instance, the authors of one study found that "8,833 out of 19,366 Ethereum smart contracts are vulnerable" to bugs such as "(i) transaction-ordering dependence, (ii) timestamp dependence, (iii) mishandled exceptions, and (iv) reentrancy vulnerability" [71]. Table 3 presents the different vulnerabilities present in smart contracts as well as detailed causes of these vulnerabilities. Atzei *et al.* proposed a taxonomy of vulnerability and categorized the different types of vulnerabilities into levels that represent the vulnerabilities: solidity, Ethereum Virtual Machine (EVM), and blockchain [85]. The vulnerability causes contract issues with codifying, security, privacy, and system performance, including blockchain scalability.

Summary And Insights:

This section discusses the security issues associated with blockchain in terms of transaction malleability. This malleability is caused because information is not immediately covered in the hash transaction. This section also discusses the issues with network security where DoS attacks are possible, privacy and confidential effects due to MitM attacks,

TABLE 3. Smart contract vulnerabilities.

Vulnerability	Cause	Smart Contract	Level	Reference
Call to the unknown	Call to the unknown	Ethereum	Solidity	[85]
Gasless send	The recipient contract's fallback function *send* is invoked	Ethereum	Solidity	[86]
Field disclosure	Selfish miners published their private chain completely.	Bitcoin	Solidity	[87]
Exception disorder	Inconsistent in terms of exception handling while the call contract will not recognize errors that occur during execution.		Solidity	[88]
Reentrancy	A call that invokes back to itself through a chain of calls.	Ethereum	Solidity	[88]
Dangerous Delegate Call	DELEGATECALL opcode is identical to the standard message call	Wallet contract, Ethereum	Solidity	[88] [89]
Time stamp dependency	Vulnerability favoring a malicious miner by changing timestamp of StartTime, EndTime		Blockchain	[90]
Block number dependency	block.blockhash function associated with block.number as parameters for random number is being manipulated			[88]
Freezing ether	Freezing ether contract i.e., no transfer/send/call/suicide code within the current contract itself to transfer ether to other address	Wallet contracts		[88]
Immutable bug	Altered contract that cannot be patched.		EVM	[91]
Ether lost in transfer	Ether sent to an orphan address which did not belong to any particular contract or user	Cryptocurrency, Ethereum	EVM	[91]
Unpredictable state	User cannot predict the state of contract if he or she invokes the particular transaction		Blockchain	[85]
Randomness bug	Biasness behavior of malicious miner by arranging their blocks to influence the outcome		Blockchain	[91]

criminal activities involving unauthorized third parties, and smart contract vulnerabilities, as listed in Table 3, caused by flaws in programming codes.

V. OTHER CHALLENGES

1) Unclear Terminology: The limited talent pool available for blockchain technology has increased the needs (both real and perceived) for regulatory agencies to ask industry experts to explain the technology and any related concerns. These needs, along with all the potential consequences of false risk analysis and its tendency to underregulate, greatly increase the risk of capture by regulators [92], [93]. In fact, even just the terms "DTL" and "blockchain" are confusing. In short, there is a general lack of technical understanding among consumers, business firms, and authorities [10], [94], [95], including in areas such as

1) the blockchain job market,
2) DTL,
3) smart contracts that require that the business logic nature in ledgers be automatically executed,
4) knowing where to look to find the necessary talent, and
5) investing in blockchain jobs regardless of the demand for new talent.

2) Risk of Adoption: Even if there are expected economic benefits, the adoption and implementation costs of DLT/blockchain for existing projects can quickly become substantial. This is particularly true for existing customers with IT systems or processes that have been written to comply with current standards, which may require costly redesigns [96]. The operational costs associated with adopting DLT/blockchain remain unclear. Still, in the short term, certain back-office processes cannot be easily removed or replaced with DLT/blockchain solutions [97], [98]. For the development of blockchain in the capital market, industry participants must consider four immediate actions:

1) evaluating the business impact and planning for the long term,
2) participating in the relevant consortium and working with regulators,
3) identifying and capturing internal ledger opportunities, and
4) implementing post-trade and manual processes (required).

3) Economic Impact: in many cases, it is unclear whether blockchain will be an improvement over centralized systems in terms of performance, throughput, scalability, security, and privacy [99]. In addition, DTL faces challenges involving economic scaling, high transaction costs, and long verification times. Besides, until a proof of concept is tried and tested, there may be uncertainty about which use cases are viable and realistic. If DTL/blockchain is not widely adopted, it will not be easy to clearly assess its broader economic impacts over the medium to long term [100]. Three areas in particular require further investigation:

1) organizational incentives and costs,
2) market environment (how cryptocurrencies are affected by demand and competitors), and
3) decision-making processes.

4) Lack of Technical Clarity: Given the ledger's decentralized nature and its function as a constant record, establishing clear governance rules is important for both authorized and unauthorized ledgers [101]–[106]. Part of the likely challenge with this governance is the result of selecting a ledger outside the contract that defines the participants' use conditions and responsibilities. Further, as part of off-ledger contracts and depending on the user's status, certain rights may not be automatically granted to the ledger user. This involves establishing procedures for specific aspects of governance, such as user identity verification, as well as establishing processes for disputing arbitration and applicable laws. It is also necessary to select a method of error correction for when incorrect data need to be added to the ledger or a transaction needs to be canceled. Specifically, with anonymous users, all approaches should focus on regulatory compliance as it relates to customer knowledge and anti-money laundering processes.

5) Regulation Uncertainty: Understanding how blockchain affects specific regulations in a wide range of regulatory environments is an important element of the development and deployment of any DLT solutions. In 2016, the company Deloitte and the Smart Contracts Alliance highlighted regulatory standpoints, approval, functions, and impacts regarding blockchain technology [99], [107]. New technology standards can be decisive, particularly with respect to the tightly regulated financial sector. According to Lamarque *et al.* [108], approximately 80% of blockchain technology focuses on business processes, while the remaining 20% focuses on technology. This imbalanced focus on the finance sector poses significant challenges for regulators attempting to decide when to intervene [109].

1) Regulatory bodies need to develop better understandings of ledger activity.
2) Regulatory uncertainty generates platform, price, and novelty risks.
3) Regulators must ensure that innovation is not suppressed while simultaneously protecting the end-user privileges.

6) Interoperable Implementations: To realize all the benefits of DLT/blockchain, ledgers must be able to exchange information with other ledgers and existing IT systems, and it is unclear whether large companies are prepared to reorganize their existing operating procedures in both the short and medium terms [101]–[103], [110]–[113]. One author emphasized the potential risk of inconsistent developments in technology, which can lead to fragmented markets [97]. Some authors have promoted enabling seamless interactions between blockchain technology and legacy systems. Meijer and Carlo [113] highlighted some implementation standards:

1) intensified conversation
2) concern about interoperability and competition in fragmented blockchains
3) common interoperability standards for different protocols, applications, and systems in areas such as cryptographic standards, interoperability standards, scalability parameters, and regulatory standards

7) Maintaining Data Privacy: Organizations should be cautious about the integrity and security of the data stored in ledgers, including both transaction data and data on the ledger's own activity [101], [103], [116], [115]. Organizations need to ensure that only people with the appropriate permissions can access the data and that any access complies with general data protection laws [114], [115]. Lamarque [109] argued that regulatory and legal intervention may be necessary to ensure that DLT/blockchain implementations can have meaningful and specific impacts.

8) Ensuring Encryption: While blockchains can provide encryption opportunities, such as having multiple copies of a book in the event of a cyberattack or computer failure, the development of access and management rights to multiple nodes represents a potential security risk, as there must be "backdoors" through which the system can be attacked [98]. Confidence in systems, verifying other users' integrity in the distributed general ledger, and consistent transaction security are some of the key challenges in increasing DLT/blockchain adoption [116], [117]. Some authors have suggested that nodes in distributed ledgers need to be able to view transaction data, even though IDT can be effectively encrypted in DLT/blockchain to validate the data. This presents a potential data privacy protection issue in certain cases of permissionless ledgers.

9) Energy-Intensive: DLT/blockchain has attracted substantial interest from technology firms, financial institutions, and other user communities. One issue with such technologies is that the ledgers are significantly more energy-intensive than centralized legacy systems [98], [101], [118]; Bitcoin blockchains, for instance, are highly energy-intensive [119]. Bitcoin uses PoW, or the number of CPU cycles a system has devoted to mining, and this is likely to represent a significant problem for future scaling that can be planned for and managed. Lamarque [108] explained that blockchain systems require considerably more energy to run than centralized ledger systems for a number of reasons:

1) more network nodes requiring unpredictable energy needs
2) many stakeholders with different approaches to blockchain technologies
3) server-side management demand
4) the need for effective cost-estimation mechanisms

10) Ambiguous Smart Contract Execution through Blockchain: There is a lack of clarity regarding whether smart contracts have been fulfilled and whether their terms can be expressed, which can limit the terms to the binary determination of whether or not the contract has been fulfilled [120]. Charles Brennan and William Lunn described how the Ethereum hack was implemented in DLT/blockchain and revealed certain flaws in smart contracts [117]. Many of the challenges associated with smart contracts stem from the lack of clarity and diverse definitions in the contracts themselves, rather than the use of DLT or blockchain technology.

Summary And Insights:

This section has discussed some more fundamental challenges that may be encountered when dealing with blockchain technology, such as the unclear terminology that is still prevalent in some regulatory agencies. Some technical understandings are clear, such as risk adoption in the capital market industry and the economic impact in many cases, yet blockchain remains unclear in terms of performance, scalability throughput, and security. In addition, there is a lack of technical clarity with clear rules from the government, and the common interoperability implementation standard and maintaining data privacy are also big challenges.

VI. EXISTING BLOCKCHAIN TECHNOLOGY SOLUTIONS

This chapter discusses some existing blockchain solutions that have been proposed in different sectors. This survey focuses on the basic theory, key attributes, features, and limitations of existing studies on blockchain solutions.

A. HEALTH CARE

Linn and Koo [121] identified simple yet robust uses of blockchain for storing patients' health data; these systems allow each patient's entire health history to be stored on an individual blockchain. The data are primarily stored in data lakes that allow for simple querying, advanced analytics, and machine learning [122]–[130]. Data lakes are simple tools for warehousing many types of data; each user's blockchain serves as an index catalog that contains a unique user identification number and an encrypted link along with timestamps to indicate the latest data modifications.

Alhadhrami *et al.* [131] also discussed how blockchains could be used in the health care sector to maintain, validate, and store data, primarily data involving consortium blockchains. These are permissible blockchains in which both the node owner and the miners have access control. Consortium blockchains work on the theory of consensus for an optimum number of validations to ensure data accuracy.

Patel [132] discussed the development of a cross-domain image-sharing blockchain network that allows for the sharing of patients' medical and radiological images based on a consensus blockchain. The author's system sought consensus among very few trusted institutions to maintain a more meticulous consensus in which less effort is needed to manage the complex security and privacy module.

There has always been a trade-off associated with using the ISN (image sharing network) developed by the Radiological Society of South America and using the proposed image sharing blockchain where the ISN uses a central authority or clearinghouse to maintain many types of incoming and outgoing access. It is also a strict network for following the average concurrency and security protocol. However, this image-sharing blockchain is an open network that can be much more vulnerable to forced attacks; the only way to secure each node's URL endpoint is to guarantee the secrecy of the private keys used to access the blockchain. Therefore, we concluded from that study that there can be several proper use cases for sharing highly sensitive data in decentralized environments. However, the security model that relies on the nodes still appears to be quite complex, based on the Federal Policies and motions of the GDPR policies.

Mettler [133] reported that there are three basic sectors of blockchain health care technology: smart health care management, user-oriented medical research, and the prevention of drug counterfeiting. In the industry of smart health care management, the author discussed the Gem Health Network, which gives providers detailed views of their patients' current medical statuses. Medical record analysis of this type leads to the creation of an ecosystem that can elucidate even the past records of a patient by transparently reducing all merit costs. Moreover, medical experts can keep track of stakeholders' activities, such as visits to physicians and health centers, to follow their treatment tracks. Such systems can contribute to insurance claims being settled faster, and the same would happen if patients were to grant insurance companies access to their relevant records.

Liang *et al.* [134] discussed the growing demand for health care devices and wearable technology along with the challenges associated with storing and maintaining patients' records; blockchain is a far more secure and optimized way of maintaining these records. The wearable devices are linked to a cloud database or network wherein all the user's data are stored. Because vast amounts of data are stored in this way, they are stored in batches in a Merkle tree, thus allowing for efficient data processing. Table 4 summarizes the existing research solutions that have been proposed for smart health care environments using blockchain technology.

Tanwar *et al.* [135] have suggested how blockchain technology led to improve transactions involving medical records in healthcare 4.0 applications. The significant advantage of using blockchain in healthcare is that it can reform the interoperability of healthcare databases, accessibility to patient medical records, prescription databases, and device tracking. Moreover, the authors have proposed an access control policy algorithm for improving medical data accessibility between healthcare providers.

Tripathi *et al.* [136] proposed a new approach for a smart healthcare system named S2HS to provide intrinsic security and integrity of the system. In this paper, two-level blockchain mechanisms are used for internal and external entities of the healthcare system. This mechanism provides isolation among different entities with consistency and transparent flow in a secured and privacy-preserved manner.

Kumar *et al.* [137] performed the simulation and implementation of a novel healthcare design using the

TABLE 4. Healthcare solutions for blockchain systems.

Reference	Proposed Scheme	Basic Theory	Attributes	Other Features	Limitations
Linn and Koo, 2017 [121]	Secure way of storing and exchanging health care data using blockchain	Secure storage of many types of medical data helpful for in-depth research	Efficiency, authenticity, availability	Provides latest accurate data for many types of health care research	Storage and data throughput, interoperability, lack of data privacy
Alhadhrami et al., 2017 [131]	Different kinds of blockchains for validating and storing health care data	Pros and cons of different blockchains for health care data	Availability, efficiency, validity, privacy	Provides optimum number of validations for maintaining accuracy	Lack of technical details, ambiguous proposed scheme
Patel, 2018 [132]	Cross-domain image-sharing blockchain system	Using the consensus of trusted organization by considering GDPR policies	Authority, privacy	Designed for extreme level of privacy and security of medical images	Lack of relevant merits for large-scale implementation. No experimental results.
Mettler, 2016 [133]	Addresses the basic sectors of blockchain technology	Usage of Blockchain sectors and its effectiveness	Effectiveness, cost saving	Looking for past details to solve the problem in the easiest way	Unclear methodology
Liang et al. 2017 [134]	Maintaining electronic health records using blockchain	User-centric system where user has all rights for sharing information	Privacy, robustness, integrity	More responsibility for the user	Limited health data sharing. Scalability issue.
Tanwar et al. 2020, [135]	Blockchain-based EHR system for health application 4.0 version	Utilizing the blockchain concept and implementing permission-based HER system with the use of chaincode concept.	Latency, Throughput, round trip time	Improving current limitations of healthcare system such as efficiency and security	Required Test bed environment, limited rounds
Tripathi et al. 2020, [136]	Proposes a blockchain-based SHS framework to provide intrinsic security and integrity	Applying two level blockchain mechanism, i.e., private blockchain for internal entities and public blockchain for internal use in health care ecosystem	Privacy-preserved healthcare system	Enable patient centric system, promotes patient mediated communication	No experimental performance
Kumar et al. 2020, [137]	Smart healthcare design, simulation, and implementation using healthcare 4.0 process	Explore optimization algorithm and improve the performance of blockchain-based decentralization system	Performance improvement, data redundancy,	Easy data maintenance	Implementation on different blockchain networks with different tools and techniques

healthcare 4.0 process. This work has explored an optimization algorithm that improves the performance of the healthcare system. The proposed method integrated the simulation-optimization process with the proposed approach and improved the performance of industry 4.0 networks and the overall system.

B. TRANSACTION SECTORS

Oh and Shong [138] provided a survey report on how blockchain technology can be used in the financial sector and how it is gaining popularity. They also defined many use cases. Blockchain in the financial industry is not substantially more technically significant than the predefined databases, but the blockchain is far superior in terms of data storage reliability. In the present structure with central authorization, if at any point a database fails, then the entire system fails, and the data can be improperly accessed and modified. However, in blockchain, such scenarios are rare because transaction data are always safe: there is no single point of failure in blockchain. The authors also provided a comparative analysis of public, private, and consortium blockchains.

Turner *et al.* [139] discussed how Bitcoin is being leveraged for malicious activities and crimes online. The biggest advantage of Bitcoin is the anonymity of transactions; all personally identifiable information is hidden in the transactions. Bitcoin users have previously been tracked through careful analysis of transaction patterns (for instance, where stolen public keys are being used). However, the issue that persists here is the usage of dark wallets or Bitcoin Fog, wherein a huge set of transactions involving a single piggy bank is released to a destination address at once. Piggy banking blockchain transactions are often maximally anonymous because it is impossible to track the recipient of the transaction. Moreover, if piggy banking is used with the Tor browsers, then the entire transaction is completely anonymous, and tracking is impossible.

Yoo [140] described the use of blockchain in financial systems where most transactions were previously centrally regulated. Previously, decentralized blockchain technology was only used in certain areas, but its use has since expanded exponentially in the financial industry; areas such as smart contracts, settlement, remittances, and securities have all come to use blockchain on some level. The R3CEV Consortium of Korea, which comprises 16 different banks, has laid the foundation of certificate authority to authenticate transactions. Moreover, transfers of funds that were previously conducted across banks through gradual gold transfers have now been reduced and partially replaced by cryptocurrency

TABLE 5. Blockchain solutions in transaction sector.

Reference	Proposed Scheme	Basic Theory	Attributes	Other Features	Limitations
Oh and Shong, 2018 [138]	Evaluation of suitability of different blockchains for finance sectors using case study	Performance-based study by using comparative analysis	Robustness, efficiency	Feasibility study for different financial institutions	Not applied to all financial institutions
Turner et al., 2018 [139]	Use of blockchain for illicit activity and how to identify it	Good technology can be used in bad ways	Robustness, effectiveness	Pattern-based behavior during transactions	Bitcoin address and IP address limited
Yoo, 2017 [140]	Development of decentralized financial system based on blockchain	Evaluate the effectiveness of blockchain	Privacy, security, efficiency	Good recommendations for finance sectors	Limited to Korean financial sector

TABLE 6. Blockchain solutions for privacy and security.

Reference	Proposed Scheme	Basic Theory	Attributes	Other Features	Limitations
Joshi et al., 2018 [141]	Summarizes the issues related to privacy and security of blockchain	Case studies for validation and recommendation	Privacy, security, effectiveness, efficiency	Optimum traceability	Lack of blockchain tools distribution and permissions
Kshetri et al., 2017 [142]	Comparison between cloud and blockchain for privacy and security	Identify the pros and cons of cloud versus blockchain	Integrity, efficiency, privacy, security	Less storage required for blockchain than cloud	-------------
Singh et al., 2019 [143]	Secure and efficient smart home architecture based on blockchain and cloud computing	Transaction handling and security analysis in smart home network	Privacy, security, confidentiality, integrity, scalability	Anomaly packet detection, high throughput, low latency	Handling limited security attacks and high execution time

transfers across institutions. Private distributed ledgers track many types of transactions between trusted authorities. The author also clearly described how the Korean banking sector could incorporate blockchain technology to increase the security and privacy of customer transactions. Table 5 summarizes the existing blockchain research solutions in the transaction sector.

C. BLOCKCHAIN FOR PRIVACY AND SECURITY

Joshi *et al.* [141] discussed the huge expansion of blockchain technology with an emphasis on the privacy and the security of the vast amounts of data involved. Blockchain transactions in the financial sector tend to be highly secure and authorized by either the central commission (in private blockchains) or the consortium of regulating stakeholders (in consensus blockchains). In the health care field, patients' medical data stored in central databases can be vulnerable to leaks, whereas blockchain architectures provide patients with full discretion over their data.

Kshetri *et al.* [142] compared how a cloud service and a blockchain operate in terms of data security and privacy. In cloud storage, it is very clear that data are not being permissioned, causing vulnerability; data are also managed and accessed by central authorities, and a rogue regulating authority can cause massive damage involving data leakage to unauthorized entities. By contrast, in blockchains, data are stored in peer-to-peer networks, and users have complete discretion over their data, thus guaranteeing complete data security and privacy.

Singh *et al.* considered the fundamental issues with smart home applications and presented a secure and efficient smart home architecture with which to overcome these challenges [143]. The proposed system also fulfills the security goals of protecting communication, scalability, ensuring the system's efficiency, and protecting against a variety of attacks. The proposed architecture incorporates blockchain and cloud computing technology in a holistic solution. Our proposed model uses the Multivariate Correlation Analysis (MCA) technique to analyze the network traffic and identify the correlation between traffic features to ensure the security of smart home local networks. The anomaly detection algorithm is presented for the detection and mitigation of DoS/DDoS attacks.

Table 6 summarizes the existing blockchain research solutions for privacy and security.

D. BLOCKCHAIN-IoT PRIVACY PRESERVING APPROACH

Yang *et al.* identified the three ways through which the location of blockchain addresses could be disclosed that raise the potential risk of privacy infringement. Therefore, the authors have proposed a novel blockchain solution to preserve the worker's position and increase the success rate of assigned work [144].

Kuo *et al.* [145] focused on developing a hierarchical approach to inherit the privacy-preserving benefits and retain blockchain adoption services concerning research networks-of-networks. Therefore, the authors have proposed

TABLE 7. Blockchain for privacy preserving scheme.

Reference	Proposed Scheme	Basic Theory	Attributes	Other Features	Limitations
Yang et al [144]	Blockchain-based location, privacy-preserving crowd- sensing system	Preserve the worker's location and increase the success rate of assigned work	Prevent re-identification, location privacy	Efficiency, security	Uploaded data can be re-used by malicious worker, quality evaluation problem
Kuo et al. [145]	Privacy-preserving model learning on the blockchain on a networks-of-networks	Implementation of hierarchical privacy-preserving model on blockchain and evaluate it on three healthcare/genomic datasets	Improve predictive correctness of datasets, improve decision support system	Learning iteration, reduce execution time,	Topology, evaluation of large number of data, advance privacy concern
Gai et al [146]	Energy trading with user's privacy using blockchain in smart grid	Differential privacy, neighboring energy trading, privacy preserving	Efficiency, user's privacy	----------------------	-------------------
Qui et al. [147]	Location privacy approach based on blockchain	Location-based service, K-anonymity	Efficiency, privacy, security	Good response time, and scalability performance increased	This method is more suitable for snapshot theory

a framework to combine model learning with blockchain-based model dissemination and with a hierarchical consensus algorithm to develop an example implementation of a hierarchical chain that improves predictive correctness for small training datasets.

Gai *et al.* [146] discussed the privacy concern caused by attackers, which use data mining algorithms to violate a user's privacy when the user group is located nearby geographically. The authors proposed a module for constructing a smart contract called the black-box module. This module allows for the regular operation of energy trading transactions per demand for privacy preservation in design objectives.

Qui *et al.* overviewed the shortcomings of two existing privacy-preserving schemes and proposed a location privacy protection method using blockchain technology. The proposed method does not require a third-party anonymizing server, instead satisfying the principle of k-anonymity privacy protection [147].

Table 7 summarizes the existing blockchain research solutions for privacy-preserving.

E. SECURITY VULNERABILITY AND TOOLS

Blockchain smart contracts offer security and privacy, but their vulnerabilities must be further understood. Here, we discuss some security tools to provide the body of knowledge necessary for creating secure blockchain software. The decentralized nature of blockchain technology carries historic immutability recognized by industries aiming to apply it in their business processes, particularly in IoT. IoT's major security issue is knowing and controlling who is connecting in huge networks without breaching privacy regulations [148].

Blockchain technology is recognized as safe in its design, but built-in applications may be vulnerable in real circumstances. For example, smart contracts have been affected financially by various unfortunate incidents and attacks. In one case, in June 2016, a reentrancy problem in split DAO caused a loss of approximately $40 million [85], and $32 million was taken by attackers in 2017 [149]. These high-profile cases show that even experienced developers can leave a system seriously vulnerable to attackers aiming to exploit security bugs in smart contracts. Table 8 presents a matrix of security tools covering the most serious vulnerabilities; as shown in the table, most of these tools address more than vulnerability. The visibility check is omitted because it is only covered by smart checks [90].

Summary And Insights:

Many existing solutions in different sectors have been discussed in this section. In the healthcare sector, various proposed schemes based on storing healthcare data improve efficiency, availability, integrity, effectiveness, and other features, while each scheme has certain limitations. Moreover, this section has also discussed the existing scheme in the transaction sector to evaluate the finance sector by using blockchain to identify illicit activity and develop a financial system. A blockchain scheme based on privacy and security is also discussed, which provides optimal traceability and anomaly packet detection.

F. ATTACK SOLUTIONS

1) LIVENESS ATTACK

To combat the active liveness attack, Conflux's consensus protocol essentially encodes two different block generation strategies proposed by Li *et al.* [150]. One is the optimal strategy that allows quick confirmation and the other is the conservative strategy that guarantees the progress of consensus. Conflux is a scalable and decentralized system with high

TABLE 8. Tools and vulnerability.

Security tool	Interface	ReEntrancy	Timestamp dependency	Mishandled exceptions	Immutable Bugs	Gas costly patterns	Blockhash usage
Oyente	Command line	✓	✓	✓	✓	……	……
Remix	Command line	✓	✓	✓	……	✓	✓
Gasper		……	……	……	……	✓	……
Securify	User interface	✓	……	✓	……	------	……
S. Analysis		……	……	✓	……	------	……
Smartcheck	User interface	✓	✓	✓	✓	✓	……
Mythril	Command line	✓	……	✓	✓	------	……

throughput and fast confirmation in the blockchain system. It uses a novel adaptive weight mechanism to combine these two strategies to an integrated consensus protocol.

2) DOUBLE SPENDING ATTACKS

To address the double-spending attack, Nicolas and Wang [151] have proposed the MSP (Multistage Secure Pool) framework which allows the pool to authenticate the transactions. The proposed framework includes four stages to overcome this attack are 1) detection stage, 2) confirmation stage, 3) Forwarding stage, and 4) broadcast stage. In addition, Begum *et al.* [152] provide a set of solutions against double-spending attacks after showing the limitation of this attack.

3) 51% VULNERABILITY ATTACK

To combat the 51% attack, Sayeed and Macro-Gisbert [153] have focused on crypto-coin with low hashing power to analyze 51% attack, revealing the weakness in the consensus protocol which makes this attack happen. The authors define the hash rate problem and provide five security mechanisms against 51% attack. A recent work that has been done to address the 51% attack includes defensive mining, implementing a "Permapoint" finality arbitration system to limit chain re-organization [154].

4) PRIVATE KEY SECURITY ATTACK

Pal *et al.* [155] have proposed public key infrastructure used in the blockchain technology to authenticate the entities to counter a key security attack. This technique ensures the integrity of the blockchain network. A group key management is discussed to secure group communication to achieve confidentiality in the network.

5) TRANSACTION PRIVACY LEAKAGE

The work proposed by Bhushan and Sharma [156] presented the overall view of security loopholes, carrying out of transactions and suggested secure transaction methodology scheme. The scheme uses a homomorphic cryptosystem, ring signature, and many other security measures to decrease the overall impact of threats to improve the reliability in the transactional process in the network.

6) SELFISH MINING ATTACK

Saad *et al.* [157] have discussed the vulnerability of self-mining and proposed a solution to counter this attack. To counter the attack, the authors leverage an honest mining practice to devise the notation of truth state for blocks during self-mining fork and also allocate self-confirmation height to each transaction. Nicolas et al [158] have done a comprehensive overview of self-mining attack and their countermeasure schemes.

7) DAO ATTACK

Ghaleb *et al.* addressed the DAO insider attack in RPL IoT network. To mitigate this attack, the authors have proposed a scheme by conducting experiments using the Contiki tool, a low-power-designed tool for resource-constrained devices [159].

8) BGP HIJACKING ATTACK

Xang *et al.* [160] proposed a BGPCoin scheme, which is a trustworthy blockchain-based internet resource solution. The scheme develops the smart contract to perform and supervise resource assignment on temper resistant Etherium blockchain. BGPCoin scheme poses a credible BGP security solution on the Etherium blockchain and smart contract programming.

9) SYBIL ATTACK

To prevent Sybil attacks in blockchain networks, Swathi *et al.* [161] have proposed a scheme to restrict the Sybil attack by monitoring other nodes' behavior and checking for the nodes which are forwarding the blocks of only a particular user.

G. COUNTERMEASURE

Although blockchain systems can be used very reliably, security mechanisms must be implemented at every point in the network. The blockchain user's private key address needs to be highly coded to make the information more secure. Blockchain network designers need to be aware of potential network attacks before implementation. Attack self-detection software must be built into the system.

This section describes existing countermeasures and detection algorithms available for technologies within the blockchain that can be used to ensure privacy and security. For a comprehensive overview of this topic, this paper extracted some existing research papers and internet resources from scientific databases. Here is a summary of state-of-the-art solutions applied to blockchain environments that address security threats and provide strong privacy.

1) QUANTITATIVE FRAMEWORK

Application: The quantitative framework is made up of two sections. While one is a blockchain simulator, another segment has a security model plan [162]. The stimulator takes after the activity of blockchain frameworks. The consensus protocol and the network are the input parameters.

Impact: The quantitative system yields a high basic procedure to check the assaults. By doing so, the framework helps build the security of the blockchain system.

2) OYENTE

Application: Oyente is built in a way that can detect bugs in Ethereum based contracts. This technology is designed to evaluate the bytecode of blockchain smart contracts on Ethereum [163]. The Ethereum blockchain system stores the EVM bytecode of smart contracts.

Impact: Oyente is very convenient to deploy on a system. It detects bugs that may be present in a system.

3) HAWK

Application: The framework is used to develop the privacy of smart contracts. The Hawk framework can allow developers to write codeless private smart contracts to enhance the security system.

Impact: Since using hawk, the developer divides a system into two main parts, financial transactions are not explicitly stored in the blockchain network system [162]. The private part stores non-public data. Financial transaction information is stored in the private part. Code and information that does not require privacy can be found in the public section [164]. Hawk protects the personal information records on a blockchain system because it uses the private smart contract that automatically generates an effective cryptographic model.

4) TOWN CRIER

Application: Town crier works by recovering data demands from clients and gather information from HTTP websites [165]. A carefully marked blockchain message got back to the client contract by the Town crier.

Impact: Town crier provides security when requesting information from clients. Strong security which is a robust model for the blockchain smart contract is provided by a local announcer/town crier.

5) LIGHTNING NETWORK

Application The Lightning network generates double-signed transaction receipts. The transaction is said to be valid after the parties involved in the transaction have signed it to accept the new check [165].

Impact: This Lightning network helps two individuals to conduct transactions between themselves without interference from a third-party miner. Double signing ensures transaction security for the parties involved.

6) SEGWIT

Application: Segwit is one of the sidechain features that runs in parallel with the main Blockchain network [166]. Signature data moves from the main Blockchain system to the extended sidechain.

Impact: By using the sidechain, more blockchain space is freed and more transactions are executed [167]. The signature data is placed in the parallel side chain in the form of a Merkle tree. With this placement, the overall block size limit has increased without interfering with the block size. Data diversification improves network security.

7) INTEGRATION OF BLOCKCHAIN WITH ARTIFICIAL INTELLIGENCE (AI)

Application: Artificial intelligence is building a machine in a way that can perform tasks that require intelligence.

Impact: Machine learning can be used by security personnel to detect anomalous behavior in the network and prevent attacks on the system [165].

8) TENDERMINT

Tendermint proposed the concept of blocking, in which security is provided by a modified reconciliation protocol based on share confirmation. Each block must be cryptographically signed by certifiers in the Tendermint consensus protocol, where certifiers are simply users who confirm their interest in the security of the system by closing their funds with the help of a bonding transaction [168].

However, some cryptographic works have been done to improve the blockchain network. For example, Wang *et al.* [169] have proposed a secure and efficient protocol using Elliptic Curve Cryptography (ECC) to solve the identity authentication issue in the smart grid. Moreover, Song *et al.* [170] have worked on security and privacy concerns for smart agriculture systems by proposing a data aggregation scheme with a flexible property that utilizes ElGamal cryptosystem. Zhang *et al.* [171] have suggested a distributed Covert Channel of the packet ordering enhancement model based on data compression to enhance the unknowability of the data. Some more work has studied the applications of providing security techniques to enhance the blockchain network system [50], [172]–[176].

TABLE 9. Solving secirity issues through blockchain characteristics.

Characteristics Issues	Smart contract	Transparent And verifiable	Decentra-lization	Anonymity	Efficiency	Persistency	Resiliency	Digital ledger
Data privacy	Yes	No	No	Yes	No	No	No	No
Access control	Yes	Yes	Yes	No	Yes	No	No	No
Single point failure	No	No	Yes	No	Yes	No	Yes	No
Third-party	No	No	Yes	No	Yes	No	Yes	No
Integrity of data	Yes	No	Yes	No	No	Yes	No	No
Availability	No	No	Yes	No	Yes	No	No	No
Immutability	Yes	No	No	No	No	Yes	No	Yes
Eavesdropping	No	No	No	Yes	No	No	No	No
Trust	No	Yes	Yes	No	No	Yes	No	No
Botnet attacks	No	No	Yes	No	No		Yes	Yes

VII. OPEN ISSUES AND RESEARCH DIRECTION

To complete our overview, we outline some open questions and research challenges, along with available requirements to improve blockchain-IoT capability. Table 9 summarizes some key blockchain characteristics that solve the security issues.

1) Vulnerability: Despite offering a robust approach for IoT security, blockchain systems are also vulnerable. The consensus mechanism based on the miner's hash power has disappeared, thus allowing attackers to host the blockchain. Likewise, it is possible for attackers to compromise blockchain accounts by exploiting private keys with limited randomness. Users need to define effective mechanisms to ensure transactions' privacy and avoid competitive attacks, leading to double spending during transactions.

2) Resiliency against combined attack: Many security solutions and applications have been discussed and proposed for blockchain-IoT, and each of them has been designed to handle certain security issues and threats. The main question involves developing a framework that can be resilient against many combined attacks with consideration of the implementation feasibility of the proposed solutions.

3) Policies for zero-day attacks: A zero-day attack is a software module technique that occurs when there is a lack of countermeasures against such vulnerability. It is difficult to identify the possibility of such attacks, and any device can be compromised by one. Most of the related suspicious activities are recognized during the development stage, but some of them are recognized during testing operations. When a vulnerability is exploited, the liabilities should be addressed by a security patch from the software distributers. A non-homogeneous Markov model is defined using an attack graph that incorporates time-dependent covariates to predict zero-day attacks.

4) Blockchain specific infrastructure: Storing the data on the blockchain database means storing information on the IoT nodes in the network that cannot be deleted. This means information is imposed on the miner nodes, which imposes huge costs on a decentralized network. Specifically, we can understand that storage-limited IoT devices may not store large blockchains that grow as blocks are added to the blockchain. It is also known that IoT devices store data on blockchains that are not useful for their transactions. Therefore, fining equipment that supports the distributed storage of large-scale blockchain-specific blockchains becomes a difficult problem. In addition, address management and basic communication protocols play important roles in the blockchain infrastructure. In particular, the reliability between devices with abundant computing resources must be established in the blockchain infrastructure. Further, the application programming interface should be as user-friendly as possible.

5) Security requirements: Considering blockchain-IoT, it is of the utmost importance for the specific condition which aims to facilitate security parameters, attack countermeasures, privacy, and trust. Blockchain-IoT must satisfy certain security requirements, illustrated as follows:

- *Secure key exchange:* It is considered as an important role in a cryptographic mechanism to secure end-to-end communications. It is a pillar of attack prevention in the network. It should be guaranteed that a key must be securely shared over the network.
- *Resource-exhausted attack resilient:* Resource exhaustion attacks are security exploitations of the targeted system or network that should be prevented. The attack can be exploited through the excessive key operation, or when many transactions occur in the network and there is abundant validation from the miners. Such attacks may cause a shutdown of the entire network.
- *Resource utilization:* The utilization of memory and power can save the operation up to a longer duration. The novel network architecture can utilize the resources well for each function in a blockchain transaction system. Some other facilities like fog computing, edge-crowd modeling, osmotic computing, and other distributed concepts can improve resource utilization and security facilities.
- *Performance trade-off:* Apart from the cryptographic requirement for providing security and efficiency, one should not ignore or compromise the system's

performance and handle the implementation overhead during parallel operation.

- *Insider threat management:* It prevents threat, combating, detecting, and monitoring of employees. Non-compromising models are required to detect and prevent false alarms in the aspects of the blockchain system.

6) Open Questions:

- How many blockchains can secure the IoT environment?
- What are the smart contract vulnerabilities, and how do smart contracts respond in the face of changing IoT environmental conditions?
- In what cases can blockchain be used in IoT networks?
- How safe will blockchain technology remain in the future age of quantum computing?
- How can the issue of latency in block creation in blockchain and cryptographic processes be addressed without compromising privacy?

VIII. CONCLUSION

The blockchain paradigm is changing the IT industry. Blockchain can bring together companies, governments, and even countries. Blockchain technology is widely recognized and highly valued due to its decentralized nature and peer-to-peer characteristics. The main takeaway of this review paper is that the authors have thoroughly analyzed several attacks on blockchain and the security issues of blockchain with some real-world examples. Moreover, this paper discussed the various security issues, challenges, vulnerabilities, and attacks that impede the increased adoption of blockchain technology while exploring these challenges in a variety of aspects. We also explained other blockchain applications and benefits, and we discussed many related opportunities at the business level. Finally, we summarized existing security solutions for different environments and open research issues.

REFERENCES

[1] Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[2] S. Singh, I. H. Ra, W. Meng, M. Kaur, and G. H. Cho, "SH-BlockCC: A secure and efficient Internet of Things smart home architecture based on cloud computing and blockchain technology," *Int. J. Distrib. Sensor Netw.*, vol. 15, no. 4, pp. 1–17, 2019.

[3] X. Jiang, M. Liu, C. Yang, Y. Liu, and R. Wang, "A blockchain-based authentication protocol for WLAN mesh security access," *Comput., Mater. Continua*, vol. 58, no. 1, pp. 45–59, 2019.

[4] Z. Deng, Y. Ren, Y. Liu, X. Yin, Z. Shen, and H. Kim, "Blockchain-based trusted electronic records preservation in cloud storage," *Comput., Mater. Continua*, vol. 58, no. 1, pp. 135–151, 2019.

[5] R. Song, Y. Song, Z. Liu, M. Tang, and K. Zhou, "GaiaWorld: A novel blockchain system based on competitive PoS consensus mechanism," *Comput., Mater. Continua*, vol. 60, no. 3, pp. 973–987, 2019.

[6] G. Sun, S. Bin, M. Jiang, N. Cao, Z. Zheng, H. Zhao, D. Wang, and L. Xu, "Research on public opinion propagation model in social network based on blockchain," *Comput., Mater. Continua*, vol. 60, no. 3, pp. 1015–1027, 2019.

[7] C. Li, G. Xu, Y. Chen, H. Ahmad, and J. Li, "A new anti-quantum proxy blind signature for blockchain-enabled Internet of Things," *Comput., Mater. Continua*, vol. 61, no. 2, pp. 711–726, 2019.

[8] W. Wang and C. Su, "CCBRSN: A system with high embedding capacity for covert communication in Bitcoin," in *Proc. IFIP Int. Conf. ICT Syst. Secur. Privacy Protection*. Cham, Switzerland: Springer, 2020, pp. 324–337.

[9] Z. Lejun, Z. Zhijie, W. Weizheng, W. Rasheed, Z. Chunhui, K. Seokhoon, and C. Huiling, "A covert communication method using special bitcoin addresses generated by vanitygen," *Comput., Mater. Continua*, vol. 65, no. 1, pp. 597–616, 2020.

[10] S. Li, F. Liu, J. Liang, Z. Cai, and Z. Liang, "Optimization of face recognition system based on azure IoT edg," *Comput., Mater. Continua*, vol. 61, no. 3, pp. 1377–1389, 2019.

[11] D.-Y. Kim, S. Dong Min, and S. Kim, "A DPN (delegated proof of node) mechanism for secure data transmission in IoT services," *Comput., Mater. Continua*, vol. 60, no. 1, pp. 1–14, 2019.

[12] L. Xu, C. Xu, Z. Liu, Y. Wang, and J. Wang, "Enabling comparable search over encrypted data for IoT with privacy-preserving," *Comput., Mater. Continua*, vol. 60, no. 2, pp. 675–690, 2019.

[13] M. A. Ferrag, A. Derhab, L. Maglaras, M. Mukherjee, and H. Janicke, "Privacy-preserving schemes for fog-based IoT applications: Threat models, solutions, and challenges," in *Proc. Int. Conf. Smart Commun. Netw. Technol. (SaCoNeT)*, Oct. 2018, pp. 37–42.

[14] A. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for IoT," *Sensors*, vol. 19, no. 2, p. 326, Jan. 2019.

[15] M. Shen, X. Tang, L. Zhu, X. Du, and M. Guizani, "Privacy-preserving support vector machine training over blockchain-based encrypted IoT data in smart cities," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7702–7712, Oct. 2019.

[16] (2019). *What is Block Decentralization*. [Online]. Available: https://lisk.io/academy/Blockchain-basics/benefits-of-Blockchain/what-is-decentralization

[17] (2015). *Obama Announces Legislation Protecting Personal Data, Student Digital Privacy*. [Online]. Available: https://www.rt.com/usa/221919-obama-privacy-student-consumer/

[18] K. Gai, M. Qiu, X. Sun, and H. Zhao, "Security and privacy issues: A survey on FinTech," in *Proc. Int. Conf. Smart Comput. Commun.*, 2016, pp. 236–247.

[19] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proc. IEEE Secur. Privacy Workshops*, May 2015, pp. 180–184.

[20] C. Cachin, "Architecture of the hyperledger blockchain fabric," in *Proc. Workshop Distrib. Cryptocurrencies Consensus Ledgers*, vol. 31, 2016, pp. 1–4.

[21] L. S. Sankar, M. Sindhu, and M. Sethumadhavan, "Survey of consensus protocols on blockchain applications," in *Proc. 4th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS)*, Jan. 2017, pp. 1–5.

[22] P. D. Filippi, "The interplay between decentralization and privacy: The case of blockchain technologies," *J. Peer Prod.*, no. 7, pp. 1–19, Sep. 2016.

[23] J. L. D. L. Rosa, V. Torres-Padrosa, A. el-Fakdi, D. Gibovic, O. Hornyák, L. Maicher, and F. Miralles, "A survey of Blockchain technologies for open innovation," in *Proc. 4th Annu. World Open Innov. Conf.*, 2017, pp. 14–15.

[24] O. Jacobovitz, "Blockchain for identity management," Lynne William Frankel Center Comput. Sci., Dept. Comput. Sci., Ben-Gurion Univ., Be'er Sheva, Isreal, Tech. Rep., 2016.

[25] (2018). *ID and Access Management: The Next Steps*. [Online]. Available: https://www.bankinfosecurity.com/interviews/id-access-management-next-steps-i-3904

[26] M. Pilkington, "Blockchain technology: Principles and applications," in *Research Handbook on Digital Transformations*, vol. 11. Cheltenham, U.K.: Edward Elgar Publishing, 2016, pp. 225–253.

[27] *Blockchain Developers*. Accessed: Dec. 2020. [Online]. Available: https://www.ibm.com/blogs/Blockchain/category/Blockchain-developers/Blockchain-open-source/

[28] S. Underwood, "Blockchain beyond bitcoin," *Commun. ACM*, vol. 59, no. 11, pp. 15–17, Oct. 2016.

[29] I. Miers, C. Garman, M. Green, and A. D. Rubin, "Zerocoin: Anonymous distributed E-Cash from bitcoin," in *Proc. IEEE Symp. Secur. Privacy*, May 2013, pp. 397–411.

[30] M. Möser, "Anonymity of bitcoin transactions," in *Proc. Munster Bitcoin Conf. (MBC)*, 2013, pp. 1–10.

Vol. 02, No. 01, pp. 29 – 40 (2021)
ISSN: 2708-0757

JOURNAL OF APPLIED SCIENCE AND TECHNOLOGY TRENDS

www.jastt.org

IoT Provisioning QoS based on Cloud and Fog Computing

Fady E. F. Samann*[,1], Subhi R. M. Zeebaree[2], Shavan Askar[3]

[1]Presidency of Duhok Polytechnic University, Duhok, Kurdistan Region, Iraq, fady.samann@dpu.edu.krd
[2]Presidency of Duhok Polytechnic University, Duhok, Kurdistan Region, Iraq, subhi.rafeeq@dpu.edu.krd
[3]Erbil Polytechnic University, College of Engineering, Erbil, Kurdistan Region, Iraq, shavan.askar@epu.edu.iq
**Correspondence: fady.samann@dpu.edu.krd*

Abstract

The wide-spread Internet of Things (IoT) utilization in almost every scope of our life made it possible to automate daily life tasks with no human intervention. This promising technology has immense potential for making life much easier and open new opportunities for newly developed applications to emerge. However, meeting the diverse Quality of Service (QoS) demands of different applications remains a formidable topic due to diverse traffic patterns, unpredictable network traffic, and resource-limited nature of IoT devices. In this context, application-tailored QoS provisioning mechanisms have been the primary focus of academic research. This paper presents a literature review on QoS techniques developed in academia for IoT applications and investigates current research trends. Background knowledge on IoT, QoS metrics, and critical enabling technologies will be given beforehand, delving into the literature review. According to the comparison presented in this work, the commonly considered QoS metrics are Latency, Reliability, Throughput, and Network Usage. The reviewed studies considered the metrics that fit their provisioning solutions.

Keywords: *IoT, QoS, Provisioning, Cloud Computing, Fog Computing, Virtualization, SDN*

Received: March 1st, 2021 / Accepted: March 29th, 2021 / Online: March 31st, 2021

I. INTRODUCTION

The growth in technological advancement has increased data generated from connected devices to the cloud. The cloud is a large data unit where computing and storing are done and made available to emphasize consumer needs [1]. The world will see a tripling of Internet-connected devices in the next decade, from 11 billion in 2019 to 30 billion by 2030 [2]. These services and software are used worldwide in various scenarios, include smart factories, intelligent farming, and cities [3]. A considerable storage size is required due to this prompt raise in data. This increase also means for data processing, a large bandwidth consumption and higher latency [4].

To enable connecting digital worlds with real worlds, the IoT has been identified as one of the enabling technologies for computing the next age. IoT applications' growth has advanced a range of fields like smart cities, smart health, connected vehicles. By 2025, the global market of IoT will reach $1567 billion, according to Statista Inc.

With this strain on the Internet today, service providers (SPs) have been between two options, either invest more in their networks or implementing stringent regulations. Both options will either lead to increase costs or not satisfying the customers. Besides, SPs are obligated to provide specific QoS according to the Service Level Agreement (SLA). That is why there is much money at stake for SPs due to the enormous excess in the numbers of devices connected to the Internet [5]. At that point, maintaining QoS while efficiently managing the network capital becomes challenging for many SPs or network operators [6].

QoS provisioning stands for the degree of quality granted to the user while carrying out a service. This definition has been receiving a significant focus over the last decades. It became a source for academia and technological solutions such as algorithms, protocols, and commercial products. However, when academia delivers a solution, either new services' criteria or growing users' standards made such a solution insufficient. For example, after thousands of contributions went into the routing area, there is still room for improvement [7].

Currently, adopting remote processing at the cloud with its first subsidiary product referred to as fog is widely agreed up on for meeting QoS requirements of IoT [8]. For this scenario, many technologies and techniques are involved such as Software Defined Network (SDN) [9- 11], Network Function Virtualization (NFV) and 5G mobile networking [12]. Moreover, due to the artificial intelligence (AI) and Machine Learning (ML) ability to solve problems and automate tasks at a

doi: 10.38094/jastt20190

network level, they become of great interest during IoT system development [13-15]. These technologies and techniques could easy-up or complicate finding the right solution for QoS provisioning in IoT systems. For the reasons above, this work's main objective is to review the most recent studies involved proposing QoS provisioning schemes for IoT systems. The next section will provide the reader with background knowledge about key concepts in the topic at hand. The surveyed studies will then be reviewed and compared with tables summarizing the utilized techniques, QoS metrics and baselines. The paper ends with giving conclusions in the last section.

II. Background and Theory

This section gives a brief epitome about the topic key concepts to comprehend IoT's characteristics and architecture with its QoS parameters. Moreover, the introduction of critical enabling technologies will also be mentioned.

A. IoT Concept and Principles

IoT is an advanced framework leveraging modern information technology. It covers a range of technological fields, such as sensor technology, integrated circuit (IC), data transmission, automation, high-end computing, information processing and security [16]. Objects can interact with one another without human involvement in IoT. The four sections of IoT industrial chain are identification, sensing, processing and data transmission [17]. These sections utilize key technologies such as Radio-frequency identification (RFID), on-chip sensor, intelligent chip and wireless communication. For example, objects with RFID tags produce radio wave identification signal detected wirelessly by RFID reader. The reader obtains the object's information and sends it to an information network system middleware through Internet or other communication channel [18]. The object names are usually represented through Object Naming Service (ONS), while Electronic Product Code (EPC) interfaces can provide other variety of object information [19]. The system's whole operation gains support from the Internet, utilizing varieties of description languages and communication protocols. Thus, it can be said that the IoT is a combination of different physical product information services based on the Internet's construction.

B. IoT Devices

Linking computers and "things" to the Internet and other networks has been a commonplace. Technological developments such as automated teller machine (ATM), wireless sensor network (WSN), machine to machine (M2M) systems and similar connections have occurred over the years. The above does not mean that all the systems and devices listed are part of what is currently known as the IoT. IoT devices are not all connected, and not all connected devices are IoT devices. The term 'Internet of Things' is used when referring to uniquely addressable things [20]. There are several IoT definitions, and it is not easy to establish a universal definition. It depends on the approach is taken, such as the technical approach, the application approach, or the business approach. However, the IoT signifies the interconnectivity and interdependence of devices with integrated sensing, actuating, and communication capabilities [21]. A thing can sense the cyber-physical surrounding to generate outcomes which upon it actuates outcomes. Then the thing share with the cyber-physical environment the outcomes that resulted from both sensing and actuating (Fig. 1) [22]. Data in IoT is collected, analyzed, organized, and communicated through hardware, software, and software systems.

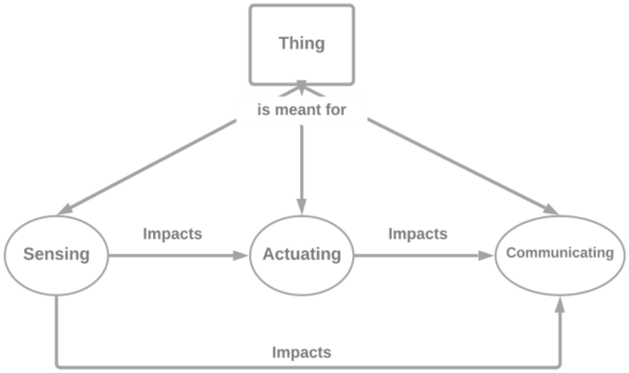


Fig. 1. Thing's duties in IoT model

C. IoT Architecture

IoT is an interconnection of intelligent things in nature and function in coordination over the network [23]. IoT's architecture concerns are network protocols, smart things, security, scalability, and interoperability through diverse devices [24]. The architecture can have three-layer as can be seen in Fig. 2 [25].

The Sensing Layer represents physically interconnected set-up monitor and maintain things remotely. Sensing is the most crucial task in the IoT system [23]. Intelligent sensor nodes and RFID are usually used for the sensing task. In this layer, RFID tags or wireless sensor nodes are designed to sense and exchange data among different things [26]. Superior technology advances IoT sensing and recognition of connecting more devices. Sensing and recognition are essential concerning networks like the IoT [27, 28].

The network layer is the second one which enables all the connected devices/things to exchange information among each other. This layer automatically discovers accessible network devices, and maps each device to a network interface. [29]. It also automatically assigns devices to their roles such as modules for deployment, work scheduling, and when needed, connecting with any other network devices. The IoT network layer's development includes dealing with network management technologies such as mobile or stationary, wireless spectrum license, security and privacy, and service recuperation [30].

The third one is the service layer. Here, IoT communicates using middleware technology that alleviates various functionalities to incorporate unstrained [31]. The main chore of the layer is to cover middleware's stipulates. Different groups industrialize these specifications. The middleware technology brings forth a cost-effective platform for IoT applications. In this platform hardware and software, schemes can be reprocessed. The service-oriented problems processed by this layer are storage administration, search engine, communications, and information transfer. Some of the service layer's components include service discovery, service composition, trustworthiness management, and services APIs [32].

The last IoT layer is the interface layer. In IoT, unalike industries and companies usually do not adopt similar network protocols [33]. Numerous issues posed in the exchange of information between different things, result from this adaption. This issue is addressed by shortening interrelation of things. Without this layer's existence, the steady increase of IoT devices will become more challenging to communicate, operate, connect and disconnect [34]. An active interface is a set of generalization services that defines the configuration between applications and services.

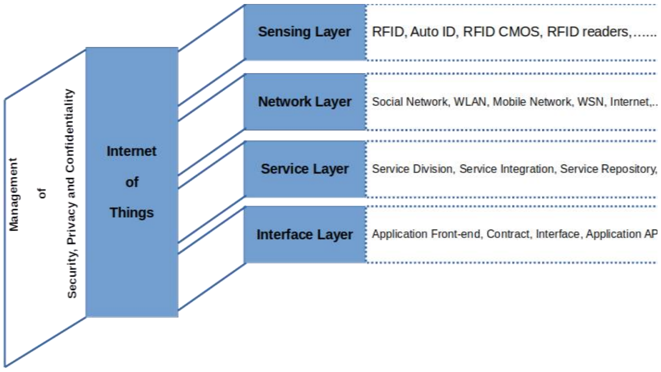

Management
of
Security, Privacy and Confidentiality
Internet
of
Things
Sensing Layer
RFID, Auto ID, RFID CMOS, RFID readers,......
Network Layer
Social Network, WLAN, Mobile Network, WSN, Internet,..
Service Layer
Service Division, Service Integration, Service Repository,
Interface Layer
Application Front-end, Contract, Interface, Application AP

Fig. 2. Illustration of IoT Architecture

D. Cloud Computing

The technology of cloud computing provides services to the user anywhere at any time [35, 36]. Here, resources are shared all around the job for speedy servicing the user. The term "cloud" comes from the different resources pool that offers services to the end-users [37]. The “computing” term refers to the computing done based on the SLA to provide the resources with efficiency to the users [38]. The aggregation of the two terms is referred to as cloud computing. Load balancing is done to increase the utilization of resources [39, 40]. However, it is considered a significant challenge in the cloud. The challenge is to distribute the computing resources effectively among the users [41, 42]. The resources are offered on-demand to meet the SLA’s requirements. Load balancing in cloud system is done through virtualization technology to effectively handle dynamic resources [43, 44]. Cloud services provided to the users can be private, public or hybrid [45, 46]. Businesses usually uses tailored private cloud for internal purposes, while public clouds are used by individuals or organizations based on their need [47]. The integration of public and private clouds provides hybrid services to the users. The SP should guarantee the QoS for each application in the data center while achieving the server’s utilization and energy efficiency [48, 49]. The cloud developers are responsible for fulfilling the users and cloud providers requirements. Lastly, cloud computing is considered a critical enabler to meet IoT applications' demand [50].

E. Fog Computing

Cisco describes Fog Computing (FC) as a cloud expansion that spread from the center to the edge to increase performance and data analytics [51]. This expansion consists of several fog nodes (FNs) distributed in various locations to provide data services and applications [52]. The FNs are each lightweight versions of the cloud server [53]. These assets provide information and processing closer to the end-devices, usually IoT. FC provides a network of collaborating units that automate storage and processing functions in real-time [54].

Moreover, the FNs' hardware and software are customizable according to the application's requirements or environment where it will be deployed [55]. FC offers localized processing services with appropriate latency for enterprises, and because the data are not standardized, the fog analyzes them locally before transmitting them [56, 57]. It executes applications locally because of the scalability and high efficiency of its data storage system. FC is not meant to compete with cloud computing but boost and strengthen cloud computing efficacy [58]. Low latency, mobility, position awareness, scalability, security, and interaction with heterogeneous devices are supported by this technology [59].

Moreover, it reduces traffic between users and the cloud and energy usage while saving the bandwidth [60]. The FNs provide computing power, storage, and networking services for the infrastructure’s applications [61]. These nodes are heterogeneous devices that range from access points, servers, edge routers, base stations, to smart end devices [51]. Scalability of FC can be internal as adding hardware or software to the node [62], or externally by adding more nodes as required to meet service provisioning. Utilizing distributed cloud service development at each node, achieving higher scalability and reliability for the system. The node's performance is influenced by the deployment location and resources allocation among the nodes [63].

F. QoS in IoT

Connecting things to the Internet is the main aim of IoT. This aim is achieved by creating a network of things that communicate with each other [64]. As IoT devices increase, the amount of data being generated would dramatically increase [65]. The devices’ capability to provide several services at once is the reason behind this increase. As a result, various factors required for QoS prediction on the user side have been elucidated [66].

The QoS service can be referred to as a quality assurance service of network connectivity, prioritizing applications across the network [22]. QoS is a crucial enabler of IoT networking because it handles network functionality, resources and offers secure connectivity. QoS systems identify traffic in order to manage delays, bandwidth, and package loss. Delivering data rapidly and with efficiency is an essential goal of IoT and its services [67]. That is why IoT needs to deliver various services and choose the right one based on QoS requirements. These requirements or metrics are diverse in IoT system because of combining things with computing and communication. There are QoS requirements for each one of these components to meet for efficient and effective IoT system. In terms of things, the IoT devices’ QoS may implicate power consumption, coverage, the optimal number of active sensors, sensor quality, data bulk, trustiness, and mobility [68- 71]. Any of the above metrics might not be significant when measured in isolation [70]. However, there is a lot more to consider when considering the vast number of devices involved in delivering the service. For example, the cumulative power consumption of hundreds of 0.9W sensors can make a real impact on the network's power usage. For communication, the network's QoS would include metrics, like throughput, response time, availability, capacity, repair time, delay and jitter [71- 74]. Relating to computing, the data analysis programming models within the cloud requires QoS metrics that satisfy throughput and response time. However, CPU usage, memory usage, network latency, and network bandwidth represent the cloud infrastructure layer's QoS requirements [70]. From the IoT application perspective, the main QoS requirements change according to the application's field. For example, a health-monitoring application requires privacy, security, precision, durability, responsiveness, robustness, accuracy, reliability and availability [68], [75, 76]. However, time-sensitive applications consider low latency as its highest priority requirement [68, 77], while high priority goes to network utilization and energy efficiency in less time-critical applications like building automation [68, 78].

III. Literature Review

The most recent and related academic works will be reviewed in this section and compared through tables in the next section.

Shaheen et al. [79] pointed out that the considerable distance among users and end-devices expand the number of routers' hops, resulting in rising latency and network utilization. Consequently, infrastructure provisioning in real-time is obstructed, and the QoS is reduced when using remote FNs for outsourced applications. A lightweight location-aware fog system (LAFF) is proposed in this work, using the fog head node model that keeps track of other FNs in terms of user registration and location. The proposed LAFF continuously improves QoS using a location-aware algorithm. In this work, the cloud layer used for data processing and storing for a longer duration. If the fog head struggles to offer user services, the cloud facilitates users. Fog heads are fixed and predetermined physically concerning the geographical region. According to the devised algorithm they worked to identify the user's location and the requested data type. Fog head knows the exact location of all FNs. If any nearest FN is unreachable, then the shortest path is found by implementing the k*-algorithm. The development of LAFF is conducting by using CloudSim to handle the simulation at the cloud, and iFogSim to handle FNs' events. Comparing to state-of-the-art frameworks, LAFF decreased latency by 11.01%, network utilization by 7.51% and service time by 14.8%. Furthermore, given RAM and CPU consumption, the proposed architecture surpasses intelligent FC analytical model (IFAM) and task placement on FC (TPFC) targeting IoT applications.

Rani et al. [80] mentioned that the challenges of densely deployed IoT networks are energy-effective communication, scalability and network coverage. The authors proposed a new IoT QoS infrastructure to combine fault tolerance and effective communication in the transmission of sensitive data. They worked on optimizing IoT's sensing layer in WSN using hierarchical and multi-hop communication protocols (ZSEP/LEACH/SEP and TSEP) to solve scalability in IoT. The network simulated in MATLAB has 200m^2 area split into four areas. In each region, a sink is used in the middle that gathers data from all the region's nodes and all four sinks forward data to the IoT's base station layer. Moreover, Cluster Heads (CHs) are chosen from within each region for data transmission between the sink and the normal node. CHs are selected according to energy levels and distance, while sinks are provided with unlimited power due to IoT restrictions. The proposed methodology was compared with CBCCP, ME-CBCCP, HCR and ERP protocols. The IoT–QoS scheme took less time for transmission than Genetic HCR and ERP. However, ME-CBCCP received the lowest time among the protocols.

Quedraogo et al. [81] stated that scaling in IoT platforms can answer the QoS requirements when the traffic load is increased. However, it would increase the provisioning costs. Their alternative answer is to scale up the network for end-to-end IoT traffic control using virtualized network functions. They relied on multi-objective optimization problem for planning network function and scaling action according to considered constraints. The planner developed by the author is called QoS for NFV enabled IoT platforms (QoS4NIP). QoS4NIP uses a Genetic Algorithm (GA) to solve the multi-objective optimization problem by making a series of improvements in an iterative process. The scaling action is implemented by deploying Traffic Control Functions (TCF) as Application Network Function (ANF) or Virtualized Network Functions (VNF) on the FNs. The TCFs were evaluated by implementing Java Management Extensions (JMX)-based monitoring tools. Results reveal that TCFs implemented as VNFs use more CPU than ANFs. However, both (ANFs and VNFs) utilize the same RAM. The authors evaluate the QoS4NIP against First-Come-First-Served (FCFS), Auto-scaling (AS), QoSEF, QoSEFe in vehicle-to-network (V2N) communication scenario which implemented in Python using Platypus library. The proposed scheme provided better end-to-end latency, excluding for traffic efficiency, where the auto-scaling scheme provided lower latency figures of 160ms.

Bhandari et al. [82] argued that Routing Protocol for Low-power and Lossy network (RPL) is not efficient for multi-purposes IoT applications which aim for diverse QoS requirements in the network. The reasons for that are the following. First, the RPL default Objective Functions (OFs) depend on a single metric, leading to trade-off in routing performance. Second, while multiple metrics are supported by RPL for parent selection, metric combinations are not defined by any specific guideline. Last reason is the RPL's design is for low data traffic network, so it suffers issues in large scale networks. Therefore, the authors proposed different OFs that ensure the discrimination of QoS at the network level. Ensuring the QoS is done by virtually dividing the physical network into instances of DODAG network topology. Different OFs can be associated with each instance and routed it through the corresponding DODAG. Moreover, a new framework for parent selection is presented in this work. It relied on the approach of multi-attribute decision making to tackle the single routing-metric issue in PRL. They resolved this issue by implementing a grey relational analysis (GRA). Three separate QoS requirements classes are identified: energy consumption, reliability and latency. Cooja simulator was used to examine the effect of network scale and data traffic load on OFs' performance in various situations. The scheme managed to show significant improvements on the QoS provision, comparing with the default RPL results. The improvements were in terms of reliability, delay, and packet loss while assuring the network's stability and minimal overhead.

Badidi et al. [83] considered selecting a fog service that ensures low latency service delivery because mapping tasks to distributed services is considered an NP-hard class problem. Thus, they presented a FC architecture based on a Fog Broker (FB) element with different scheduling algorithms. The broker receives inquiries from various applications and upon available fog services resources provide a scheduling plan for the different tasks. The application's inquiries are sent to the FB by assigning it with a collection of appropriate FNs to meet their QoS requirements. CloudAnalyst simulation tool simulated a fog cluster scenario with five FNs as proof of concept. This tool utilizes three scheduling policies to determine fog service efficiency. Three broker scheduling policies provided by CloudAnalyst, and they are Reconfigure Dynamically with Load (RDL), Optimise Response Time (ORT) and Closest Fog Node (CFN). According to the results, the average request service time was no more than 2ms for all cluster nodes and the scheduling policies. Consistent average request servicing time across cluster FNs allowed by the CFN scheduling policy. The ORT scheduling policy had the shortest time for average request servicing on almost all FNs.

Badawy et al. [84] mentioned that a dynamic service-oriented environment is essential to meet the QoS requirements while satisfying the user demands. Moreover, in the long run, IoT complex services will suffer from performance debasement and real-time adaptive sensing. Thus, relying on the Backtracking Search Optimization Algorithm (BSOA), they designed a dynamic QoS Provisioning Framework (QoPF) for service-oriented IoT. The QoPF's main objective is to optimize complex service quality in the IoT application layer through balancing service reliability with a reasonable computational time cost. Assessed, intrinsic and perceived QoS are three QoS models classified by the authors. The performance metrics used to evaluate the framework efficacy are throughput, jitter, delay time, and packet delivery ratio. NS2.35 simulator was used for evaluation, while the benchmark algorithms were GA, PSO, ACA and Differential evolution (DE). The BSOA significantly outperforms all the benchmark algorithms for all metrics except the packet delivery ratio metric against PSO algorithm.

Asad et al. [85] argued that the QoS parameters might differ between the access network and the core network. Furthermore, network-based QoS provisioning schemes usually require the end-devices to inform the network devices about their QoS requirements. To tackle the points mentioned above, the authors developed a QoS aware selection scheme for multi-radio access technologies (M-RAT). The IoT nodes with M-RAT can connect to one or more AP simultaneously. For optimal access device selection, the optimization problem runs separately at each node. The problem had four constraints. First constrain is to ensure the parameters considered for QoS provisioning satisfy the predefined thresholds. The second one is to limit the number of access devices that a node can connect to simultaneously. Constrain number three limits the number of nodes that can connect to an access device. The last one limits the workload at the access devices from all connected nodes. Mixed-integer linear programming (MILP) and binary possibilities were used to solve the problem. The Mininet emulation environment was used because it requires low computing power. The proposed scheme's performance was compared to best-SNR and maximum bandwidth selection methods in average throughput and delay. The results illustrated that the proposed scheme was closer to the ideal system than the others in terms of throughput. However, it was closer to the best-SNR selection method in terms of delay.

In another work by Asad et al. [86], the authors also worked on a QoS aware selection scheme for a M-RAT client. They found by reviewing the literature that the selection techniques are only client-centric RAT or network-centric QoS provisioning. Thus, they presented a novel hybrid end-to-end QoS provisioning technique that combines client-centric and SDN based network-centric approaches. The proposed architecture for the QoS scheme has four layers. The first layer is the end-devices layer that contains clients with M-RAT. The second one is the access layer for M-RAT access devices. The fourth layer composites from SDN controllers. The core layer is the last one where interconnecting devices such as routers are responsible for carrying data between networks. The core-QoS algorithm is implemented in the controller layer. The access-QoS algorithm implemented by the client device to select an access device by a single parameter. On the other hand, the core network's minimum cost path is calculated by the core-QoS algorithm according to the client's requirements. Mininet-WiFi network emulator was used to emulate a scenario of an indoor wireless LAN network with two WiFi APs. Moreover, two Raspberry Pi 4 equipped with 2.4GHz IEEE 802.11ac network interface cards were used in an experiment as WiFi APs, while three Android-based smartphones and a tablet used as end-devices. The emulation results showed that the proposed methods outperformed the AP selection approach based on the Received Signal Strength Indicator (RSSI) in the hardware experiment.

Ali et al. [87] considered ensuring QoS for IoT mission-critical application or services while providing wireless channel access to every connecting object. Accordingly, accommodating the demand for IoT over a limited wireless spectrum is a new challenge for communication. This work's primary focus is priority differentiation among secondary users (SUs) in cognitive Radio IoT. The authors worked on reducing high priority SU call blocking probability and increasing channel utilization efficiency. Thus, they developed a scheme for priority-based call admission and channel allocation by using traffic-aware dynamic channel reservation. First, they surveyed the available licensed channels based on the traffic patterns of its primary users. Second, for queuing analysis, the SU traffic rate is estimated by a Markov Chain model. According to it, the channels are reserved for each priority. The workflow of the scheme is as the following. Different SU application with different priorities contacts the secondary base station (SBS) which decide to block or allow the channel allocation. Here the allocation is based on priority class and the total available channel, which detected according to the primary user (PU) traffic activities probability. The proposed scheme's performance was evaluated and compared with greedy non-priority and fair proportion schemes in call-blocking, call-dropping, channel utilization and throughput. According to simulation results, the proposed priority scheme surpasses the baseline schemes. However, the baseline schemes' figures fell between the four priority classes for the SU application suggested by the authors.

Yousefpour et al. [88] introduced a framework for QoS-aware Dynamic Fog Service Provisioning (QDFSP) and called it FOGPLAN. It is based on dynamically deploy application services on FNs, or releasing previously deployed ones on FNs to meet QoS requirements while minimizing cost. Dynamically placing fog services on either FNs or cloud servers has an essential effect on network utilization and end-to-end delay. The framework does not make any assumptions about IoT devices' capabilities. Integer Nonlinear Programming (INLP) formulation and two greedy algorithms were used to address the optimization problem of QDFSP. The proposed framework's performance evaluation was done through simulation of real work traffic traces and a Discrete-Time Markov Chain (DTMC)-based traffic generator. The asymptotic complexity was the same for both minimum-delay and minimum-cost algorithms. However, according to the results, minimum-cost is faster than the minimum-delay algorithm, particularly for more FNs and services case. Except for the optimum execution reached by INLP, minimal-delay algorithm had the lowest average operation delay and average delay violations. It was concluded that minimum delay output comes at a slower run-time rate.

Yao et al. [89] addressed the failure issue during virtual machines (VMs) renting by fog provisioning to manages tasks and reduce device cost. Scaling VMs should boost reliability and QoS, but it will increase device cost. The authors investigated reliability maximization while reducing the system cost for providing fog resources in IoT networks. They formulated an Integer Linear Programming (ILP) problem. However, it suffered from complex computation. Thus, another algorithm was designed to accomplish sub-optimal solutions with improved time efficiency. Fog resource provisioning formulated as a multi-objective problem, then converted into a single-objective problem by weighted sum method. The principle here is that the different computing tasks of IoT devices are offloaded to the FN. Then the FN schedules these tasks to be processed on several VMs. The authors designed a Modified Best Fit Decreasing (MBFD) algorithm to attain sub-optimal solutions for the scheduling problem. MBFD was simulated in MATLAB, and the outcomes were compared against the the IBM CPLEX Optimizer's optimal solution. Moreover, they benchmarked the proposed algorithm with another from a past work called (Bench), which only considered the system cost. The simulation demonstrated that MBFD provides near-optimal solutions. However, it performed similarly to the Bench algorithm in terms of reliability.

Yao et al. [90] also worked on leasing and releasing VMs by the FN in an on-demand fashion. They focused on power management to sustain stable wireless transmission rate and acceptable QoS. This work addresses jointly optimize the number of rented VMs and power management problem for system cost minimization whilst guarantee QoS requirements. The Mixed-Integer Non-Linear Programming (MINLP) to formulate the optimization problem. Then it was converted to a convex optimization problem solved by the gradient projection algorithm through relaxing its integer variables. An adequate solution is obtained by an integer recovery scheme. The proposed system architecture consists of FN connected to IoT gateway and mobile IoT devices, that move within the gateway's coverage. The proposed QoS scheme was simulated and compared with the problem's lower bound. The convex problem is solved to obtain the bound after relaxing the number of rented VMs at a given location. The comparison was also made with a Fog Provisioning Problem (FPP) scheme that selects a fixed transmission power during the connection period. According to the outcomes the proposed algorithm performed similarly to the relaxed MINLP's lower bound and surpassed the FPP scheme.

Verma et al. [91] considered the hot-spot problem in multi-hop communication among the IoT-based Wireless Sensor Network (WSN). This issue occurs when the nodes nearest to the sink node get burdened by the other nodes' traffic data. Thus, they presented two QoS provisioning-based routing protocols based on multiple WSN-based IoT sinks. The authors called them Optimized Energy and Threshold Sensitive Stable Election Protocol (O-ETSSEP), and Multiple data Sinks-based Optimized-ETSSEP (MSO-ETSSEP). They relied on energy threshold, residual energy, distance and node density variables for optimizing Cluster Head (CH) selection in both protocols. For network energy balancing, the protocols use three energy heterogeneity levels. Also, MSO-ETSSEP uses four data sinks along each square-shaped network periphery to minimize hot-spot problems by surrounding multi-hop communication. MATLAB simulations evaluated the protocols through considering multiple scenarios. The QoS provisioning performance metrics were; stability period, network lifetime, network efficiency, networks remaining energy, throughput, latency and reliability. The performance of O-ETSSEP was validated against the TSEP38 and ETSSEP protocols. MS-ETSSEP and MS-SEP were compared against the MSO-ETSSEP. The results pointed out that integrating multiple data sinks into the network improves its reliability and stability. Moreover, the observed increase in performance of the MSO-ETSSEP was related to the proposed selection of CH and it achieved enhanced stability compared to MS-ETSSEP and MS-SEP.

Srinidhi et al. [92] utilized the multi-objective optimization problem to approximate the network's outage performance and lifetime. They combined quantum particle swarm optimization (QPSO) and improved non-dominated sorting genetic algorithm (NGSA) to produce Hybrid Energy Efficient and QoS Aware (HEEQA) algorithm. The HEEQA algorithm is designed to balance the devices by tuned MAC layer parameters to reduce energy consumption. To solve the multi-objective optimization problem, NSGA was applied, while the QPSO algorithm is used to get the best suitable combination. This work stress more on finding equilibrium between network lifetime and QoS provisioning. NS-2 simulator was used to evaluate the HEEQA algorithm, which compared to the QPSO. The comparison's metrics were the maximizing residual energy, end-to-end delay, packet delivery ratio (PDR), transmission overhead, maximizing network lifetime and throughput. Tuning up of MAC layer parameters reduced energy consumption of each node in the IoT network. The HEEQA outperforms QPSO in terms of all performance metrics. However, it could perform poorly in energy conservation when nodes are mobile with different moving speeds.

Li et al. [93] discussed that spectrum shortages contributed to the changing of spectrum use from an exclusive to a sharing mode due to the increase of wirelessly connected IoT. However, it is not easy to assure QoS while using a shared spectrum due to its unpredictable availability. Thus, the authors suggested metric that guarantee the QoS statistically by evaluating how much data can be delivered during a session period via a shared band, and called it probabilistic link capacity (PLC). A Distributionally Robust (DR) data-driven approach was developed based on the first and second-order statistics to estimate the PLC's value. The DR-PLC was formulated into a semi-definite programming problem based on the worst-case conditional-value-at-risk (CvaR) to calculate it for each case. Accordingly, a service-based spectrum aware data transmission scheme was designed to satisfy the various IoT service by allowing efficient use of different spectrum. They also proposed a network model named a cognitive capacity harvesting network (CCHN), that ease the IoT data transmissions over a shared spectrum. This architecture aimed to enhance the existent cellular network by transforming it into an ultra-dense network similar to the 5G design. It includes Macro-cell Base Station (MBS), femtocell Base Station (FBS), and Cognitive Radio Router (CRR). Finally, it was numerically evaluated and compared the PLC under different probability distribution and DR-PLC for under exact data-driven statistics or uncertain ones. According to the results, PLC and DR-PLC cannot accomplish similar confidence levels, while the gap among them becomes more extensive due to historical data fluctuations. DR-PLC provided an efficient way to insure QoS while utilizing the shared spectrum.

Khan et al. [94] considered the security of the relay nodes in multi-hop communication while assuring QoS. They suggested a secured communication scheme that is QoS-aware (QoS-IoT). The scheme is based on a Sybil attack detection mechanism for identifying compromised nodes and their counterfeit identities. The scheme selects an optimal contention window (CW) after detection to efficiently utilize the available bandwidth and achieve per-flow fairness. The detection mechanism is a signal-print based on the node's obtained signal strength information to detect malfunctioning nodes. The size of CW depends upon the actual to fair bandwidth allocation ratio. The Binary Exponential Back-off (BEB) mechanism was used to select the optimal CW. The proposed scheme is based on the following network model. An area of 100x100m^2 was split into smaller IoT networks, where each one dwell of static, mobile, Sybil and high-powered nodes. Thus, only delay and throughput were considered as QoS requirements because they are deeply affected by Sybil nodes' existence. The Sybil nodes block actual or genuine nodes from the use of network services with various forged identities. The network model is simulated in NS-2. The scheme was evaluated and compared with First-In-First-Out (FIFO), Round Robbin (RR) scheduling, and Cross-layer based on Utilization evaluation to Contention Window (CUCW) schemes in terms of throughput, fairness and the utilization of link. By increasing the offered load, the QoS-IoT received better fairness index compared to the other schemes. However, it performed similarly to CUCW in term of throughput. The QoS-IoT received smaller queue length by increasing the offered load than the other schemes.

Guo et al. [95] stated that queueing delay is nun-negligible in IoT applications due to the scarce edge server's computation resource. They also argued that due have workload at the edge of the network, the cloud energy consumption can be lower than in the edge servers. Therefore, to achieve green computing while providing QoS for end-users, they formulated a problem for the Delay-Based Workload Allocation (DBWA). The problem is based on optimal workload allocation between local edge, neighboring edge-servers, and the cloud to reduce energy consumption while guaranteeing the delay. A DBWA algorithm was proposed for solving the problem and it was based on the theory of Lyapunov drift-plus-penalty. The proposed scheme's network model was structured as IoT devices pushing computation jobs stochastically to a layer of edge nodes containing edge servers and edge communication infrastructures to connect to the cloud layer. The edge nodes make workload allocation decisions to offload the arrival jobs to a neighbor edge or the cloud or execute it locally. The ping-pong effect was avoided by not offloading already offloaded jobs again. The event-based simulator combines MATLAB and C++ to simulate a scenario with three IoT-devices regions, three edge nodes and the cloud. The scheme is compared with the edge-only and cloud-only offloading versions. The DBWA surpassed the other energy consumption schemes and obtained average end-to-end delay by increasing job generation rate or size.

End-to-End Delay (E2ED) estimators are significant for designing efficient QoS provisioning scheme for IoT systems. Therefore, Maslouhi et al. [96] proposed real-time evaluation metrics and addressed varying packet payload (PP) size effects in multi-hop wireless IoT networks through counting hops from source to destination. The authors considered the following four elements (Radio propagation delay, Transmission delay, Queueing delay and Signal processing delay) that contribute to the end-to-end packet delay in one direction from source to destination in their theoretical study. IP6, IP4 and ATM network protocols evaluated in terms of packet transmission delay vs packet number. Because of E2ED strongly dependent on the message size, this work concentrates on the message's average length and header. In MATLAB simulation, the IoT wireless network is considered and a single source node is transmitting packets to a single destination node across several IoT nodes. The results are compared with Ethernet's use and the speed of the Internet using fixed values. According to the results, the estimator provided reasonable estimates of payload packets, End-to-End delay and jitter. Thus, it provided valuable insight into multi-hop wireless networks' QoS provisioning.

To optimize sharing resources among IoT services, Skarlat et al. [97] presented a system model called fog landscape. It consisted of fog cells, fog colonies, and a FC management system. Fog colonies are micro data centers that are created by the accumulation of fog cells. Each fog colony has a control node that provision resources by coordinating fog cells. Also, it communicates with other colonies to coordinate extra resources if needed. The colonies connect to a middleware running in the cloud called FC management system. Also, the authors introduced the Fog Service Placement Problem (FSPP) scheme to address the placement of IoT services on virtualized fog resources. The placement considered QoS constraints such as deadlines on the execution time of applications. FSPP was implemented as an ILP problem and solved using IBM CPLEX solver. The solution was evaluated in terms of the execution cost and QoS support. The fog landscape environment was simulated using iFogSim, and the FSPP was compared to execution in the cloud. According to the results, 70% of services were utilized when FSPP included in the fog-landscape. This lead to a 35% reduction in the execution cost comparing to the execution in the cloud. The application's deadline was not violated by the FSPP scheme, unlike the baseline approach.

Muralidharan et al. [98] mentioned a promising paradigm to handle the exponential increase in the global IoT traffic volume, called Named Data Networking (NDN). The NDN traditional version only supported PULL traffic, where interest pulls Data packets from the IoT devices. However, PULL traffic as well PUSH traffic is required by IoT applications. For effective exchange of data in IoT applications, the authors presented a hybrid PUSH-PULL Traffic (PPT) model that uses NDN's efficient qualities to amend the IoT QoS parameters. The NDN's data exchange model is altered to push data as soon as IoT devices generate it without the need to remain online and check for an inbound request. The authors define the taxonomy of the network model as three entities. The IoT devices are smart sensors that can name Data packets. IoT gateway delivers messages and works as a point for entering and exiting from a network to another one. The third entity is the NDN cache router (CR) to hold and execute the proposed PPT algorithm. A Building Management System (BMS) was considered by this work in a smart building to evaluate the proposed model's performance. The simulations implemented in Visual C/C++ and the PPT model results were compared with traditional NDN and IPv6 protocol. PPT results showed that the generated network load is 50% lower than the IPv6. This helped deliver almost 98% of the packets. Also, the PPT model was 50% higher than the IPv6 in terms of average throughput.

IV. Discussion and Comparison

The technologies and techniques used by the surveyed studies will be discussed and compared in this section. At the end of this section, three comparison tables for the reviewed studies that focused on QoS provisioning for IoT. Table I present the problems considered by the surveyed studies and the techniques used for solving them. Table II summaries the considered QoS metrics with the corresponding references. The third table includes the baseline algorithms or approach considered by the corresponding authors in their evaluation. The solutions presented by all the mentioned studies addressed their legit corresponding problems. According to the comparison table (Table I), the commonly used QoS metrics were Latency, Energy efficiency, Throughput, Availability and Reliability. However, the reviewed studies did not settle on using all the metrics mentioned in the background knowledge section. Instead, each one used the metrics that fit their provisioning solutions. Moreover, some studies introduced their metrics, usually a combination of fundamental QoS metrics [93, 94]. Some works were done on ready protocols or standards such as PRL and NDN to make them more feasible for provisioning QoS in IoT system [82, 98]. In terms of the network model, most of the reviewed studies relied on FC paradigm to propose their schemes [79, 81, 83, 88- 90, 97]. The reviewed studies also included provisioning schemes for IoT environments that needed resources allocation for NFV [81, 89, 90, 97]. These studies shared with the other ones, the necessity to solve objective optimization problems, which usually done by linear or nonlinear integer programming [86, 88]. However, others used a Markov chain model to formulate their problems [87], [88]. Towards modern communication techniques, a selective number of studies designed QoS provisioning schemes for IoT devices with M-RAT or the ability to share the spectrum [85-87, 93]. Two studies out of the reviewed studies focused on multi-hop communication, while one considered security during designing the QoS provisioning scheme [91, 94]. Finally, comparing the solutions' effectiveness presented in the reviewed papers is out of the scope of this work. However, this is difficult to do because the authors considered different baselines and QoS metrics.

TABLE I. Problems and Techniques Considered by Recent Studies that Focused on QoS Provisioning for IoT

Ref.	Problems	Techniques
[79]	The distance among users and end devices increases the number of routers/hops, resulting in higher latency and network utilization	A lightweight location-aware fog system (LAFF) based on fog head node model
[80]	The challenges of densely deployed IoT networks are energy-efficient communication, network coverage and scalability.	Optimize IoT's sensing layer in WSN using hierarchical and multi-hop communication protocols (ZSEP/LEACH/SEP and TSEP) to solve IoT's scalability.
[81]	Scaling in IoT platforms can answer the QoS requirements when the traffic load increases, but it would increase the provisioning costs.	Scaling up the network for end-to-end IoT traffic management using VNF.
[82]	RPL protocol is not efficient for multipurpose IoT applications	Virtually dividing the physical network into instances of DODAG network topology. Each instance can be associated with the different objective function.
[83]	Selecting a fog service that ensures low latency service delivery because mapping tasks to distributed services is considered an NP-hard class problem.	a FC architecture based on a fog broker element with several scheduling algorithms
[84]	In the long run, IoT complex service will suffer from performance degradation and real-time adaptive sensing.	A Dynamic QoS provisioning framework (QoPF) for service-oriented IoT based on BSOA algorithm
[85]	IoT's heterogeneous characteristic causes the QoS requirements to differ from one IoT node to another	a QoS aware selection scheme for IoT nodes with multi-radio access technologies (RAT)

[86]	Past literature focused only on network-centric QoS provisioning or client-centric RAT.	A novel hybrid end-to-end QoS provisioning technique that combines client-centric and SDN based network-centric approaches.
[87]	Accommodating the demand for IoT over a limited wireless spectrum is a new challenge for communication	A scheme for priority-based call admission and channel allocation by using traffic-aware dynamic channel reservation.
[88]	Ensuring Quality of Service (QoS) for delay-sensitive complex applications is challenging.	A framework for QoS-aware Dynamic Fog Service Provisioning (QDFSP) called FOGPLAN.
[89]	Fail issue during VMs renting by fog provisioning to manages tasks and reduce device cost.	Formulating reliability maximization while reducing the system cost to provide fog resources in IoT networks using ILP problem
[90]	The QoS may be degraded for the power limited mobile IoT devices because the conditions of the wireless channel are not consistent.	Jointly optimize how many VMs can rent and power control problems for system cost minimization while ensuring QoS requirements.
[91]	The hot-spot problem in multi-hop communication among the IoT-based Wireless Sensor Network (WSN).	Two QoS provisioning-based routing protocols based on multiple WSN-based IoT sinks. They called them Optimized Energy and Threshold Sensitive Stable Election Protocol (O-ETSSEP), and Multiple data Sinks-based Optimized-ETSSEP (MSO-ETSSEP).
[92]	Reducing energy utilization in industrial IoT network without compromising the QoS.	Combining quantum particle swarm optimization (QPSO) and improved non-dominated sorting genetic algorithm (NGSA) to produce Hybrid Energy Efficient and QoS Aware (HEEQA) algorithm.
[93]	The challenge of ensuring QoS while using a shared spectrum due to its unpredictable availability	A Distributionally Robust (DR) data-driven approach was developed based on the first and second-order statistics to estimate the value of probabilistic link capacity (PLC).
[94]	Ensuring the security of the relay nodes in multi-hop communication while assuring QoS.	a QoS-aware secured communication scheme (QoS-IoT) based on a Sybil attack detection mechanism for identifying compromised nodes and their counterfeit identities.
[95]	Achieve green computing while providing QoS for end-users is a challenge	A Delay-Base Workload Allocation (DBWA) algorithm based on Lyapunov drift-plus-penalty theory
[96]	Accurate and efficient End-to-end delay (E2ED) estimators are significant for designing efficient QoS provisioning scheme for IoT systems.	A real-time evaluation metrics and addressed varying packet payload (PP) size effects in multi-hop wireless IoT networks through counting hops from source to destination.
[97]	Optimizing sharing resources among IoT services by using FC	Fog Service Placement Problem (FSPP) scheme designed to address the placement of IoT services on virtualized fog resources
[98]	The exponential increase in the volume of global IoT traffic	A hybrid PUSH-PULL Traffic (PPT) model uses NDN's efficient qualities to amend the IoT QoS parameters.

TABLE II. QoS Metrics Considered by Recent Studies that Focused on QoS Provisioning for IoT

QoS metrics	Reference
Latency	[79, 81, 82, 84 - 86, 88, 91 - 97]
Network Usage	[79, 87, 91 - 94, 97, 98]
Service Time	[79, 83, 97]
RAM Consumption	[79]
CPU Utilization	[79]
Stability	[80, 91, [94]
Scalability	[80, 88]
Energy efficiency	[80, 82, 90, 93, 95]
Throughput	[81, 82, 85, 87, 91-94, 98]
Availability	[81, 86- 88, 90- 92]
Reliability	[82, 84, 87- 93, 96, 98]
Response Time	[83, 97]
jitter	[84, 96]
Device/Network Cost	[88- [90, 97]

TABLE III. Evaluation Baselines Considered by Recent Studies that Focused on QoS Provisioning for IoT

Ref.	Baselines
[79]	Intelligent FC Analytical Model (IFAM) and Task Placement on FC (TPFC) model
[80]	CBCCP, ME-CBCCP, HCR and ERP protocols.
[81]	First-Come-First-Served (FCFS), Auto-scaling (AS), QoSEF, QoSEFe
[82]	Default RPL
[83]	Optimize Response time (ORT), Closest Fog Node (CFN), and Reconfigure Dynamically with Load (RDL).
[84]	GA, PSO, ACA and Differential evolution (DE) algorithms
[85]	best-SNR and maximum bandwidth selection methods
[86]	the Received Signal Strength Indicator (RSSI) AP selection approach
[87]	Greedy non-priority and fair proportion schemes
[88]	All IoT's requests to the cloud and Static Fog approach where the services are deployed statically at the beginning
[89]	The IBM CPLEX Optimizer's optimal solution and Bench algorithm.
[90]	The problem's lower bound acquired by solving the convex problem through relaxing the number of rented VMs at a given location and fixed transmission power approach.
[91]	O-ETSSEP is performed versus the ETSSEP and TSEP38 protocols, while MSO-ETSSEP compared against MS-ETSSEP and MS-SEP.
[92]	QPSO algorithm
[93]	PLC under different probability distribution (normal, uniform and Gamma distribution)
[94]	First-In-First-Out FIFO, Round Robbin (RR) scheduling, and Cross-layer based on Utilization evaluation to Contention Window (CUCW) schemes
[95]	Edge-only and cloud-only offloading approaches
[96]	IP6, IP4 and ATM network protocols
[97]	Execution in the cloud.
[98]	Traditional NDN and IPv6 protocol

V. Conclusion

All the mentioned studies had legit problems to solve, and they addressed it with brilliant solutions. According to Table II, the commonly considered QoS metrics are Latency, Reliability, Throughput, and Network Usage. However, these studies did not settle on using all the metrics mentioned in the background knowledge section. Instead, each one used the metrics that fit their provisioning solutions. Moreover, most of the reviewed studies considered FC paradigm as their network model for the proposed schemes which required resources allocation for NFV. Finally, due to the IoT system's heterogeneous characteristics, the metrics for QoS provisioning cannot be unified. Thus, there is no one solution fits all cases. To conclude, the academic community will still have many cases to go through while new communication technologies are coming up or still in the pipeline, such as LiFi and 6G.

References

[1] B. Paharia and K. Bhushan, “Fog Computing as a Defensive Approach Against Distributed Denial of Service (DDoS): A Proposed Architecture,” in 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Jul. 2018, pp. 1–7, doi: 10.1109/ICCCNT.2018.8494060.

[2] N. H. Mahmood et al., “White Paper on Critical and Massive Machine Type Communication Towards 6G,” arXiv, Apr. 2020, [Online]. Available: http://arxiv.org/abs/2004.14146v2.

[3] I. Sittón-Candanedo, R. S. Alonso, S. Rodríguez-González, J. A. García Coria, and F. De La Prieta, “Edge Computing Architectures in Industry 4.0: A General Survey and Comparison,” in Advances in Intelligent Systems and Computing, vol. 950, 2020, pp. 121–131.

[4] I. S. Abdulkhaleq and S. Askar, “Evaluating the impact of network latency on the safety of blockchain transactions,” Int. J. Sci. Bus., vol. 5, no. 3, pp. 71–82, 2021, doi: 10.5281/zenodo.4497512.

[5] A. V. Bataev, I. Zhuzhoma, and N. N. Bulatova, “Digital Transformation of the World Economy: Evaluation of the Global and Russian Internet of Things Markets,” in 2020 9th International Conference on Industrial Technology and Management (ICITM), Feb. 2020, pp. 274–278, doi: 10.1109/ICITM48982.2020.9080392.

[6] A. Constantin and I. B. Bacîș, “Performance targets and QoS requirements for the service provided to users/subscribers of public IP networks,” in Advanced Topics in Optoelectronics, Microelectronics and Nanotechnologies X, Dec. 2020, no. December 2020, p. 32, doi: 10.1117/12.2570968.

[7] M. Molnár, “QoS Routing for Data Gathering with RPL in WSNs,” in Advances in Intelligent Systems and Computing, vol. 1132, 2020, pp. 87–111.

[8] E. Ahmed, I. Yaqoob, A. Gani, M. Imran, and M. Guizani, “Internet-of-things-based smart environments: state of the art, taxonomy, and open research challenges,” IEEE Wirel. Commun., vol. 23, no. 5, pp. 10–16, Oct. 2016, doi: 10.1109/MWC.2016.7721736.

[9] S. Askar, “SDN-Based Load Balancing Scheme for Fat-Tree Data Center Networks,” Al-Nahrain J. Eng. Sci., vol. 20, no. 5, pp. 1047–1056, 2017.

[10] F. S. Fizi and S. Askar, “A novel load balancing algorithm for software defined network based datacenters,” in 2016 International Conference on Broadband Communications for Next Generation Networks and Multimedia Applications (CoBCom), Sep. 2016, pp. 1–6, doi: 10.1109/COBCOM.2016.7593506.

[11] G. Aziz and S. Askar, “Software Defined Network Based VANET,” Nature, vol. 5, no. 3, pp. 83–91, 2021, doi: 10.5281/zenodo.4497640.

[12] P. Krishnan, S. Duttagupta, and K. Achuthan, “SDN/NFV security framework for fog-to-things computing infrastructure,” Softw. Pract. Exp., vol. 50, no. 5, pp. 757‑800, May 2020, doi: 10.1002/spe.2761.

[13] H. Song, J. Bai, Y. Yi, J. Wu, and L. Liu, “Artificial Intelligence Enabled Internet of Things: Network Architecture and Spectrum Access,” IEEE Comput. Intell. Mag., vol. 15, no. 1, pp. 44–51, Feb. 2020, doi: 10.1109/MCI.2019.2954643.

[14] C. M. Mohammed and S. Askar, “Machine Learning for IoT HealthCare Applications : A Review,” Int. J. Sci. Bus., vol. 5, no. 3, pp. 42–51, 2021, doi: 10.5281/zenodo.4496904.

[15] K. D. Ahmed and S. Askar, “Deep Learning Models for Cyber Security in IoT Networks: A Review,” Int. J. Sci. Bus., vol. 5, no. 3, pp. 61–70, 2021, doi: 10.5281/zenodo.4497017.

[16] M. A. M.Sadeeq, S. R. M. Zeebaree, R. Qashi, S. H. Ahmed, and K. Jacksi, “Internet of Things Security: A Survey,” in 2018 International Conference on Advanced Science and Engineering (ICOASE), Oct. 2018, no. October, pp. 162–166, doi: 10.1109/ICOASE.2018.8548785.

[17] S. I. Saleem, S. R. M. Zeebaree, D. Q. Zeebaree, and A. M. Abdulazeez, “Building smart cities applications based on IoT technologies: A review,” Technol. Reports Kansai Univ., vol. 62, no. 3, pp. 1083–1092, 2020.

[18] L. M. Haji, O. M. Ahmad, S. R. M. Zeebaree, H. I. Dino, R. R. Zebari, and H. M. Shukur, “Impact of cloud computing and internet of things on the future internet,” Technol. Reports Kansai Univ., vol. 62, no. 5, pp. 2179–2190, 2020.

[19] H. Aftab, K. Gilani, J. Lee, L. Nkenyereye, S. Jeong, and J. Song, “Analysis of identifiers in IoT platforms,” Digit. Commun. Networks, vol. 6, no. 3, pp. 333–340, Aug. 2020, doi: 10.1016/j.dcan.2019.05.003.

[20] K. Ali and S. Askar, “Security Issues and Vulnerability of IoT Devices,” Int. J. Sci. Bus., vol. 5, no. 3, pp. 101–115, 2021, doi: 10.5281/zenodo.4497707.

[21] H. Raad, Fundamentals of IoT and Wearable Technology Design. Wiley, 2020.

[22] A. Qamar, M. Asim, Z. Maamar, S. Saeed, and T. Baker, “A Quality-of-Things model for assessing the Internet-of-Things’ nonfunctional properties,” Trans. Emerg. Telecommun. Technol., Jun. 2019, doi: 10.1002/ett.3668.

[23] L. Da Xu, W. He, and S. Li, “Internet of Things in Industries: A Survey,” IEEE Trans. Ind. Informatics, vol. 10, no. 4, pp. 2233–2243, Nov. 2014, doi: 10.1109/TII.2014.2300753.

[24] P. P. Ray, “A survey on Internet of Things architectures,” J. King Saud Univ. - Comput. Inf. Sci., vol. 30, no. 3, pp. 291–319, Jul. 2018, doi: 10.1016/j.jksuci.2016.10.003.

[25] T. Poongodi, A. Rathee, R. Indrakumari, and P. Suresh, Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm, vol. 174. Cham: Springer International Publishing, 2020.

[26] S. Fosso Wamba, A. Anand, and L. Carter, “A literature review of RFID-enabled healthcare applications and issues,” Int. J. Inf. Manage., vol. 33, no. 5, pp. 875–891, Oct. 2013, doi: 10.1016/j.ijinfomgt.2013.07.005.

[27] J. Guerrero-Ibáñez, S. Zeadally, and J. Contreras-Castillo, “Sensor Technologies for Intelligent Transportation Systems,” Sensors, vol. 18, no. 4, p. 1212, Apr. 2018, doi: 10.3390/s18041212.

[28] Z. J. Hamad and S. Askar, “Machine Learning Powered IoT for Smart Applications,” Int. J. Sci. Bus., vol. 5, no. 3, pp. 92–100, 2021, doi: 10.5281/zenodo.4497664.

[29] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, “A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications,” IEEE Internet Things J., vol. 4, no. 5, pp. 1125–1142, Oct. 2017, doi: 10.1109/JIOT.2017.2683200.

[30] E. Borgia, “The Internet of Things vision: Key features, applications and open issues,” Comput. Commun., vol. 54, pp. 1–31, Dec. 2014, doi: 10.1016/j.comcom.2014.09.008.

[31] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, “Middleware for Internet of Things: A Survey,” IEEE Internet Things J., vol. 3, no. 1, pp. 70–95, Feb. 2016, doi: 10.1109/JIOT.2015.2498900.

[32] M. A. A. da Cruz, J. J. P. C. Rodrigues, J. Al-Muhtadi, V. V. Korotaev, and V. H. C. de Albuquerque, “A Reference Model for Internet of Things Middleware,” IEEE Internet Things J., vol. 5, no. 2, pp. 871–883, Apr. 2018, doi: 10.1109/JIOT.2018.2796561.

[33] P. Gokhale, O. Bhat, and S. Bhat, “Introduction to IoT,” Int. Adv. Res. J. Sci. Eng. Technol., vol. 5, no. 1, pp. 41–44, Jan. 2018, doi: 10.17148/IARJSET.2018.517 41.

IoT in Banking: The trends, threats, and solution

Mardiana Abu Hassan, Nur Azaliah Abu Bakar, Noor Hafizah Hassan

Razak Faculty of Technology and Informatics,
Universiti Teknologi Malaysia,
Kuala Lumpur, Malaysia
mardiana.ah@graduate.utm.my; azaliah@utm.my;
noorhafizah.kl@utm.my

Article history

Received:
10 May 2021

Received in revised form:
15 May 2021

Accepted:
25 May 2021

Published online:
26 Jun2 2021

*Corresponding author
azaliah @utm.my

Abstract

The Internet of Things is the next step of the digital revolution that will change consumers' lives. The Internet of Things promises to be a worthy representative of an open course in technology, economics, and culture. IoT, without a doubt, has a promising future. The modern consumer actions and uses represent inescapable digital transformations for banking institutions. Emerging digital world developments guide all banking services' digital transformation. However, the security threats of using IoT in banking are increasing. Cybercriminals such as hacking, corruption, and financial violence, data breaches, and financial expenditure risks will continue to trouble the use of IoT in banking. Therefore, this research aims to study the banking industry's existing IoT uses, issues, and challenges adopting the IoT in the banking industry. IoT threats are highlighted in this paper. This article sets out a model dimension of the process monitoring framework for IoT security risk management. Other than that, this paper also studies the existing security risk management model of IoT in banking. Moreover, preventive IoT protection initiatives and approaches to enhance IoT protection by implementing blockchain technology and Control Model Information Structure are addressed in this article

Keywords: *banking, digital trends, internet of things, risk assessment, security threats*

1. Introduction

Interconnected devices, also known as the internet of things (IoT), encompass the networked interconnection of everyday objects. They are all equipped with ubiquitous intelligence [1]. There are many and substantial consequences from such a corpus of technologies; indeed, the IoT increases the internet's ubiquity by integrating objects with interaction capability [2]. The Internet of Things promises to be a worthy representative of a forthcoming revolution in technology, economics, and culture. IoT, without a doubt, has a promising future[2, 3].

The modern consumer actions and uses represent inescapable digital transformations for banking institutions. Thus, emerging digital world developments guide all banking services' digital transformation. These two changes will probably upgrade the old paradigm of banking services that we know, leading to a new type of related banking system, the first brick to transform digital banking. However, the security threats of using IoT in banking are increasing. Cybercriminals such as hacking, corruption, and financial violence, data breaches,

* *Corresponding author. azaliah @utm.my*

and financial expenditure risks will continue to trouble the use of IoT in banking[4, 5].

This paper presents a methodology to encourage an IoT system's safety analysis using nearly fully automated threat modelling and risk evaluation processes. The proposed method relies on a modelling approach to architectural aspects of the IoT system components and their safety features. It enables identifying threats, risk assessment, and selecting appropriate countermeasures to mitigate existing risks. Therefore, our primary research goal is to study the banking industry's existing IoT uses, issues, and challenges adopting the IoT in the banking industry. IoT threats are also highlighted in this paper. Other than that, this paper also studies the existing security risk management model of IoT in banking. Moreover, preventive IoT protection initiatives and approaches to enhance IoT protection by implementing blockchain technology and Control Model Information Structure are addressed in this article.

2. Related Works

Visualise a world where all digital objects can share information and interact. Connected objects can also communicate through the internet and other communication networks with their user. The diversity of IoT interrelation globally will strike 25 billion by 2025. Kevin Ashton at the Massachusetts Institute of Technology (MIT) first came up with the term "Internet of Things" in 1998 and interpreted it as "allowing people and things to be interconnected with any time, anyplace, anything and anyone, typically using any path or network and any services" [6].

IoT has developed in five phases. The first phase is creating the World Wide Web by connecting two computers. The third phase is related to the mobile internet, which connects mobile devices and the internet. The fourth phase is people-internet explaining about the connection enabled by social networks. They advanced to the IoT for globally linked objects [7]. Figure 1 depicts the evolution of IoT Evolution of the Internet in five phases.

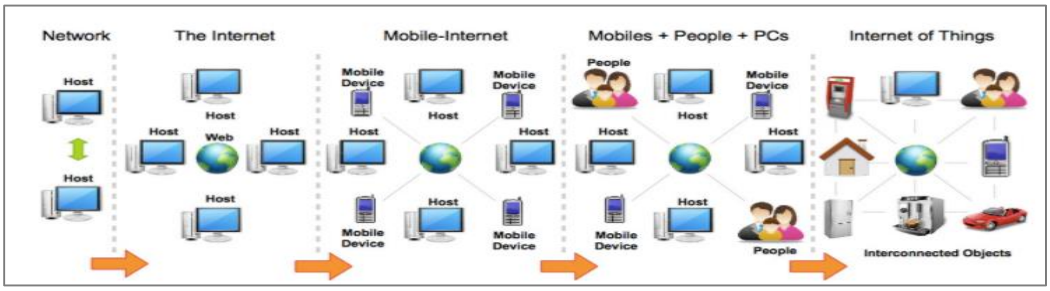


Figure 1. Evolution of Internet of Things [7]

Internet evolution starts with the connection of two computers and then moves towards creating the World Wide Web by connecting many computers. The mobile internet came into being through mobile devices' link to the internet. Then, through social networks, people's identities have joined the internet. Finally, it moves towards the Internet of Things that connects objects to the internet every day.

The IoT overgrowing and it influenced daily life. Interconnected devices are unquestionably a step towards new applications in many sectors of the economy. Service industries such as banking, insurance, transportation would primarily benefit from the rapid, automated processing and sharing of huge data quantities. Consequently, it will promote new business models of sophisticated networking for connected devices.

2.1 IoT in Financial Services

Interconnected devices are unquestionably a chance for banks to remain competitive. Consumers today expect from the Bank and, in particular, the new digital one a great deal of innovation that will provide them with adequate service in their new connected lifestyle[4]. Below we describe six digital developments using IoT, directly affecting financial services.

i. Mobile Banking

Consumers are now demanding fast, easy and instant access to all banking services in this digital age. IoT allows users to use digital devices to access their bank account anytime and anywhere. Presently, most of all digital devices are design with biometric characteristics. Biometrics recognise people's unique physical, behavioural characteristics. It enables access to mobile banking services from any digital device. Currently, E-Wallet is steadily growing, and e-wallet may help users reduce fraud as the data stored in the e-wallet is encrypted [4, 5].

ii. Virtual Money

Blockchain is an advanced technology that will track in the coming years. Many economic sectors could be revolutionised, beginning with banking and insurance. Customer can use securely and without central control to store and communicate information. It appears to be some data repository containing all user exchanges since its inception. The blockchain can be used in three respects: to transfer assets such as currency, securities, improved asset traceability, and automatic contract execution of "smart contracts." It also can be used on IoT platforms to face digital challenges as an analytical model tracking that records the data generated during IoT, ensuring protection through sharp identification rules and finally instant payments among devices and network members[8-10].

iii. Personal Financial Management (PFM)

The PFM solutions kit offers the customer a summary of all the flows from his accounts. Using IoT-generated data, PFM tools can help banks deliver personalised and more targeted services to their customers[11]. Hence, IoT is required to produce notifications to monitor customer usage.

iv. Know Your Customer (KYC)

KYC is using by financial institutions for identification and customer knowledge. Banks apply KYC procedures because it prevents fraud and money laundering. These statistical data can be linked to marketing uses[11, 12]. The IoT integrated with the digitalisation of identity will change customers' financial behaviour to provide related services and products.

v. Cyber Criminality

Financial institutions offer innovative solutions to secure banking transactions. One of the examples of this solution is Multi-Factor Authentication (MFA). MFA is one of the best methods to increase authentication assurance for consumers' confidential web, servers, machines, and mobile applications. Connected devices usually employ multi-factor authentication with a password used in conjunction with a time-boxed token that the staff possesses, push notification to a mobile app, or biometrics[5, 11].

2.2 IoT Challenges and Issues in Banking

Even though IoT would greatly benefit the banking and financial institutions, there are still significant challenges that need to be considered and resolved before adoption in those environments.

i. Data Breach

Data breaches, especially data that contain sensitive intelligence information, can pose a threat. Bank holds valuable information and top confidential data. If this information is breached and made available, it can exploit to initiate multiple social engineering attacks. Data tempering can also be a way to illegally obtain data that contribute to data leakage or data breach[13, 14].

ii. Complex Infrastructure

Above mentioned, IoT is an interconnected device through a network. Many people find it difficult to understand what IoT technologies are all about because they are quite complex to use. When connected through a network, all of the previously mentioned technologies make it possible for them to interact and influence one another. However, when the interaction is broken and a single device removed, the formed system may ultimately break down and lead to huge losses[15]. The main reason that financial and banking institutions shun the use of IoT technology is that many are unwilling to use hardware led by companies they are unaware of and then use programming companies they have never heard of before[11].

iii. No Standard Operating Procedure for Maintainance

There are different types of IoT hardware equipment, including home devices and industrial equipment[13, 16]. They are created by different kinds of manufacturers and require other maintenance requirements. There would be problems caused by a universal standard that can hinder how these devices function and can only be solved if there is only one seller or distributor of these IoT devices. Even then, monopolisation will severely negatively impact the worldwide economy.

2.3 IoT Threats to Banking

The effects of a cyberattack on a banking institution can be horrendous. This threat can also have explosive consequences. Without implementing strong security measures, banking institutions would continue to face the threat of cybercrimes. That estimate is likely inaccurate, as IoT expenditures were expected to increase once vendors gain a clearer understanding of security and privacy risks associated with the IoT[17, 18]. More IoT decision-making will include security spending in the future because of people's awareness of smart devices' vulnerability to hacks.

Some risks are associated with the increase in IoT in the banking industry, such as data capacities always pose a threat to cyber criminals[13]. The sophistication of IoT infrastructure has allowed tremendous information to be collected. For example, intelligent sensors have been used in machine learning to collect data to increase organisations' value[19]. Furthermore, confidentiality in the IoT setting is always questioned. Regardless of whether insurance is used to validate details, digital aggressors' success is critical[12]. Banking institutions have been the target of device theft from various groups such as hackers, cybercriminals.

These devices, such as laptops and mobile phones, are easy to target because they are small, handy, and easy to remove quickly. The price of stolen laptops, mobile phones, and other handheld electronic devices is not just on the replacement cost. The cost of equipment and accessories, the software installed, the cost of configuring replacement software, and the cost of lost time for the owner while the device replaced[20]. But the more significant cost that a bank has to bear is the potential data leakage and liability resulting from lost confidential valuable, and top-secret intelligence information[18].

Many IoT in financial services devices will be targets for cybercriminals because of the personal information collected and payment capabilities created by the objects[21]. Since financial companies do not control this information, it's vulnerable to threats. Customers must know what data gathered and how they will use it. Top innovations in the banking industry include the following but not limited to:

i. Banking on wearables

Wearable gadgets have been the most influential banks until now, owing to a developing biological system of devices and a generally simple beginning. Many banks now allow credit card credit to watch Apple Watch and Fit Pay applications. Numerous banks are utilising their very own wristbands to offer some contact-free instalments[22].

ii. Proactive service

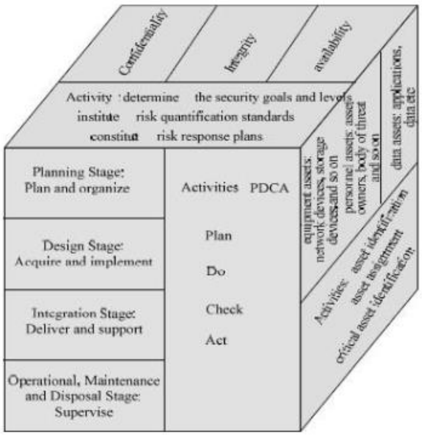
IoT will substantially enhance monetary and financial administrations' ability to change a financial product or administration choices effortlessly. Suppose there is any uncertainty or concerns about an item. In that case, it can be spotted easily, and the issues resolved as fast as possible. Advisors are also pleased to get past examples to clients, and they manage them accordingly. This development of modern accounting tools can help improve companies' operations [21].

iii. Banking at home

Capital One in the United States currently makes it possible for customers to pay their bills through Amazon's Alexa, yet this is by no means the only retail managing account association to do so, nor will it be the last. Take UK challenger bank Starling, for example, trying different things with Google Home, coordinating its API with a smart speaker to empower clients to bring equalisation issues and instalments through voice directions[23].

2.4 McCumber Cube Security Management Model

John McCumber created a model framework for establishing and evaluating information security (information assurance) programs, known as The McCumber Cube. This security model is depicted as a three-dimensional Rubik's Cube-like grid, as shown in Figure 2.


Confidentiality
Integrity
availability
Activity :determine the security goals and levels
institute risk quantification standards
constitute risk response plans
Planning Stage: Plan and organize
Design Stage: Acquire and implement
Integration Stage: Deliver and support
Operational, Maintenance and Disposal Stage: Supervise
Activities PDCA
Plan
Do
Check
Act
equipment assets: network devices, storage devices and so on
personnel assets: asset owners, body of threat and so on
data assets: applications, data etc
Activities: asset identification
asset assignment
critical asset identification

.

Figure 2. McCumber Cube Security Management Model[24]

i. S-dimension

S-dimension governs the stability and operation of the information system. The S-Dimension aims to protect information systems and activities' reliability, privacy, and accountability. The tasks about management priorities of the S-Dimension include:

1) Risk-taker will define the IoT software and security policies.
2) To initiate risk qualification criteria.
3) Reinforce risk management preparedness.

ii. R-dimension

The R-dimension features support the scale, including infrastructure and associated events. Data management tools include network and storage units, network properties, wealthy owners, and offending organs for private properties and documents and software for computer properties.

iii. P-dimension

P-dimension is an approach that regulates the dimension. The process of preparation, start-up, the architecture of the information system life cycle is carried from the threat risk assessment and monitoring process.

This study adopts this model to design the IoT Security Risk Management Process for the banking industry.

3. Methodology

The lack of an integrated threat model to IoT systems that can consider the specific characteristics of all possible components of a complex IoT infrastructure is also a problem. This shortage makes it very difficult for actual IoT deployments to perform an efficient security evaluation. Although the literature is quite generous about threats to specific alternatives and technologies, a complete and consistent list of threats applicable to a system to be deployed on production is difficult to find. Finally, the key players involved in the setup and implementation of an IoT device must be considered. It is worth noting that these tasks are mostly assigned to technicians without particular experience because it is often not economically feasible to include highly trained and costly security experts. For instance, implementing a smart home device is linked to the provider's home network and provides total control over the building. While this opens up a great deal of danger, a trained security professional is not involved in configuring such a device at implementation.

We propose a modelling approach based on the ISO standards guidelines to address such issues. This model allows us to build a threat model for a particular IoT system deployment in a semi-automated way and support safe design activities by establishing a range of security measures to mitigate existing ones. In particular, security countermeasures are indicated in security controls defined in the NIST Security Control System. It is quickly and easily accessible to map other existing structures, making our method versatile and easy to reuse in various contexts. The methodology introduced in this study makes almost completely automatic threat modelling and risk evaluation of IoT systems following the standard IoT features. The suggested methodology illustrated in Figure 3

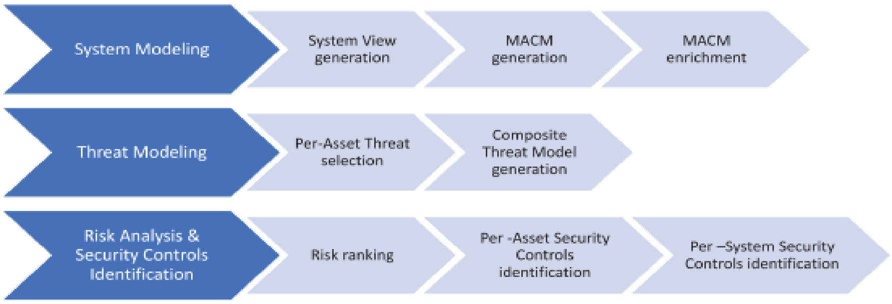

System Modeling
System View generation
MACM generation
MACM enrichment
Threat Modeling
Per-Asset Threat selection
Composite Threat Model generation
Risk Analysis & Security Controls Identification
Risk ranking
Per -Asset Security Controls identification
Per –System Security Controls identification

Figure 3. IoT automated risk analysis methodology

Figure 3 comprises three key steps:

1) System modelling is intended to evaluate the IoT system to define the key assets to secure and model them properly.

2) Threat modelling focuses on the detection of device threats.

3) Risk analysis and security control are intended to estimate each perceived hazard and identify countermeasures to mitigate current safety control risks.

5. Proposed Work

There are many advantages of using IoT in the banking sector. For example, there are numerous types of IoT wearable banking equipment produced by various manufacturers and need a different maintenance approach. A defect in IoT functionality can result from the lack of a standard. While every manufacturer agrees to use basic standards, it is always important to fix technical problems. Besides, IoT has allowed wealth management application, alarming consumers if their account is targeted[18].

However, IoT will produce vast data and additional costs to maintain and safeguard them. Organisations do not have IoT data testing systems available for errors and omissions. Therefore data quality is not always accurate. IoT allows the banking sector to makes any payment. As a result, technology allows for a stable and controlled international trade environment in which all payments are handled via an intelligent sensor network and connected devices. IoT should also be the main protective regulator[18]. As IoT adoption continues to expand, researchers are also developing a range of reference architectures, structures, guidelines, mechanisms, and standards relevant to IoT.

With a rapidly growing number of IoT systems with an increased number of things and devices, a more significant number of interactions will take place. These new connected devices would use the internet as a communication resource. This will trigger several challenges, as most of the stored data on central servers in IoT systems are preserved. Only those devices which are connected to the centralised network can obtain the data from the servers. The majority of IoT systems are implemented using a centralised server approach. IoT systems collect information from the sensor devices, focusing the data such that it is appropriately transmitted to the server through a wired or wireless network or the internet.

Correspondingly, the existing internet infrastructure's processing capabilities may not be supported effectively for the large-scale IoT system. Expansion in the internet infrastructure must manage the vast data processed in large-scale IoT systems. The best solution to do this is to have decentralised or distributed networks where Peer-to-Peer Networking (PPN), Distributed File Sharing (DFS), and Autonomous Device Coordination (ADC) functions can be used[25].

This study will clarify the value of selecting a blockchain technology solution. Blockchain technology offers a better solution to improve the IoT security in IoT systems. Blockchain can perform these three functions, allowing IoT systems to track many connected and networked devices. BC allows IoT systems to process transactions between coordinated devices. BC will enhance IoT systems' privacy and reliability, making them more robust[26]. BC allows peer-to-peer messaging faster with the distributed ledger's help, as shown in Figure 5.

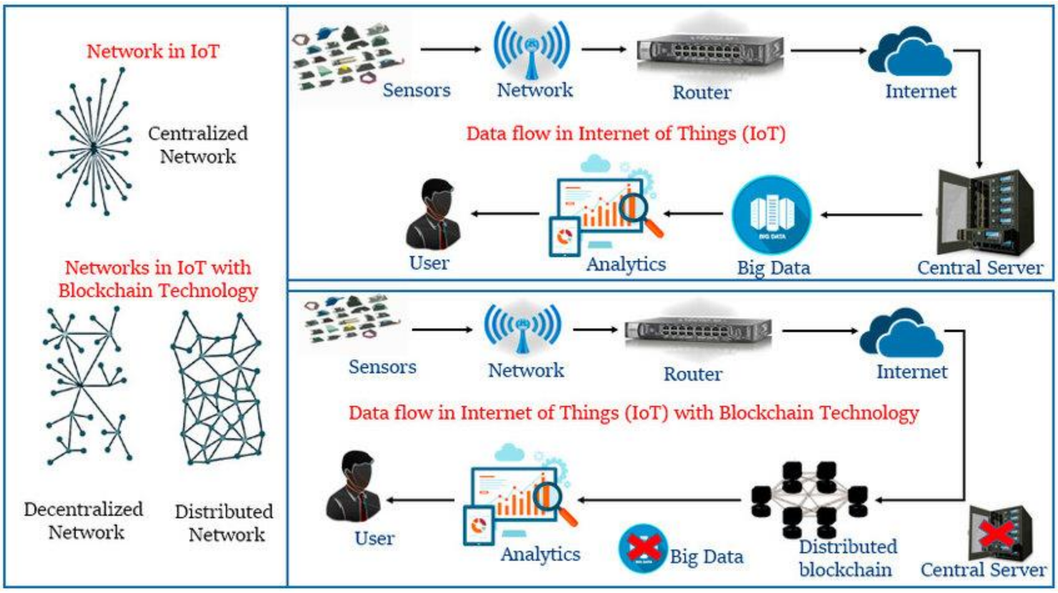


Figure 4. IoT with Blockchain Technology[26]

The IoT data flow process with BC technology is different from the IoT system alone. In IoT with BC, the data flow is from the sensor-network-router-internet-distributed blockchain-analytics-user. Here, the distributed ledger is tamper-proof that does not allow incorrect interpretation, incorrect authentication of the data. BC complexly eliminates single thread communication (STC) in IoT to make the system more trustless. With BC's adoption in IoT, the data flow will become more reliable and secure[5, 26].

The next suggestion to propose the Banking IoT Security Risk Management Model is by adopting the McCumber Cube Security Management Model. Organisations should identify the vulnerabilities and drawbacks of the risk management model, and they should always get ready to face the emerging security conditions. Several solutions have been designed to ensure the risk is still in the range outside the IoT environment. Figure 6 depicts an improved risk management model proposed by the abovementioned researchers. There is 3 phase involved in this proposed model.

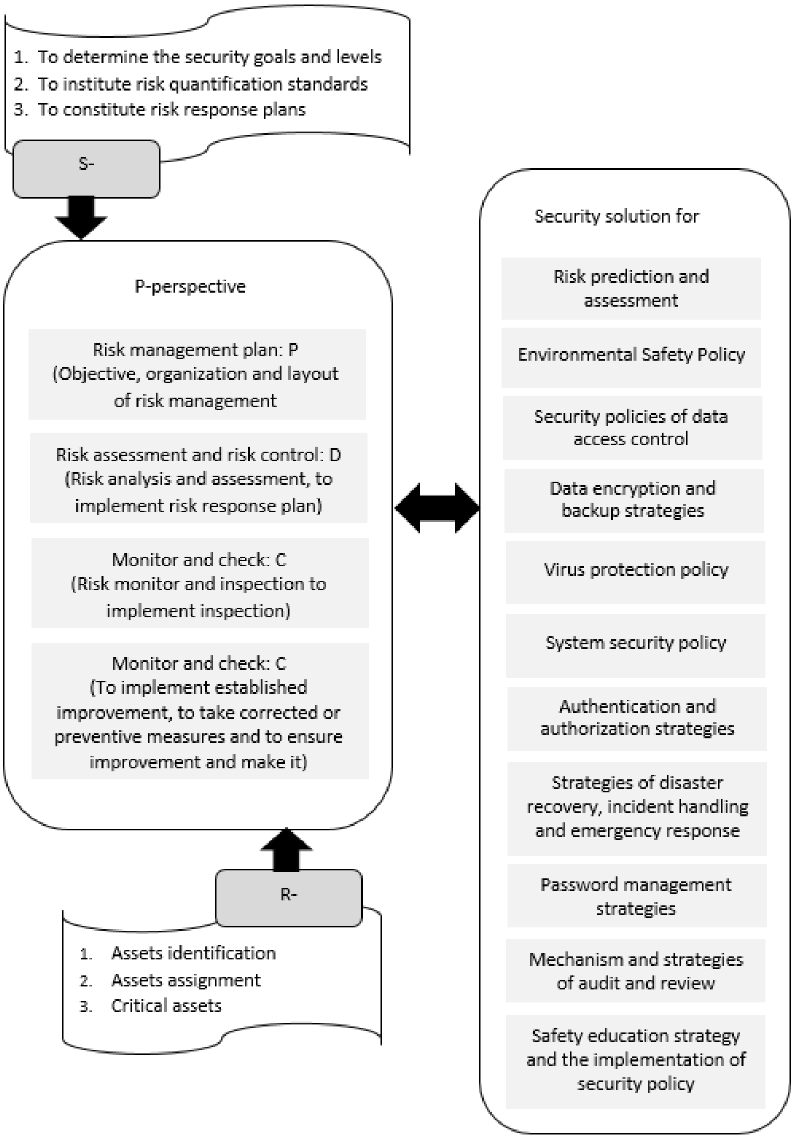

1. To determine the security goals and levels
2. To institute risk quantification standards
3. To constitute risk response plans
S-
P-perspective
Risk management plan: P (Objective, organization and layout of risk management
Risk assessment and risk control: D (Risk analysis and assessment, to implement risk response plan)
Monitor and check: C (Risk monitor and inspection to implement inspection)
Monitor and check: C (To implement established improvement, to take corrected or preventive measures and to ensure improvement and make it)
R-
1. Assets identification
2. Assets assignment
3. Critical assets
Security solution for
Risk prediction and assessment
Environmental Safety Policy
Security policies of data access control
Data encryption and backup strategies
Virus protection policy
System security policy
Authentication and authorization strategies
Strategies of disaster recovery, incident handling and emergency response
Password management strategies
Mechanism and strategies of audit and review
Safety education strategy and the implementation of security policy

Figure 5. Proposed Risk Management for Banking

i. R-Viewpoint – Protecting Information Assets

R-Viewpoints focuses on protecting information assets as *"any software, hardware, data, administrative, physical, communications, or personnel resource within an information system."* This phase is vital to determine, implement, and enhance information assets' security in organisations to maintain their cash flow, competitive strategies, and identity.

ii. S-Analysis – Analyse application goals

While S-Analysis focuses on risk assessment for strategic objective, market purpose, security purposes, and enforcement objective, by designing policies and procedures based on internal risk tolerance and document workflows, banks should be ready for any form of cybercriminal attacks.

iii. P-Perspective -A lifecycle approach

P-Perspective look at the risk assessment at various life cycle stages. Centralise IoT control for events across functional silos both inside and outside the banks' glass walls to ensure simple, coordinated and automated responses. This centralisation allows stakeholders to have a single view on the "risk," the "bad thing," or "what is affected," which assists departmental leaders in making informed decisions about projects to minimise their effect on them. Hence the P-Perspective follow the Plan-Do-Check-Act (PDCA) steps to ensure its secured process is in place.

6. Conclusion

Our goals are to safeguard the IoT by proposing a framework contrary to a collective solution. This paper presents a methodology to encourage an IoT system's safety analysis using nearly fully automated threat modelling and risk evaluation processes. Moreover, the proposed methodology relies on a modelling approach to architectural aspects of the IoT system components, and their safety features have been introduced. It enables identifying threats, risk assessment, and selecting appropriate countermeasures to mitigate existing risks.

The future work will focus on IoT-related compliance, including current compliance, best practices and the review of recent attempts to regulate IoT in general. As IoT adoption continues to expand, many reference architectures, structures, guidelines, mechanisms, and standards relevant to IoT are also developing to enhance IoT security. This study had clarified the value of selecting a blockchain technology solution as blockchain technology offers a better solution to improve the IoT security in IoT systems.

Acknowledgments

These should be brief and placed at the end of the text before the references.

References

[1] S. Akter, K. Michael, M. R. Uddin, G. McCarthy, and M. Rahman, "Transforming business using digital innovations: The application of AI, blockchain, cloud and data analytics," *Annals of Operations Research*, pp. 1-33, 2020.

[2] Y. Velayutham, N. A. A. Bakar, N. H. Hassan, and G. N. Samy, "IoT security for smart grid environment: Issues and solutions," *Jordanian Journal of Computers and Information Technology*, vol. 7, no. 1, pp. pp. 13-24, 2021.

[3] N. A. Bakar, W. M. W. Ramli, and N. H. Hassan, "The internet of things in healthcare: an overview, challenges and model plan for security risks management process," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 15, no. 1, pp. 414-420, 2019.

[4] A. Alti and A. Almuhirat, "An Advanced IoT-Based Tool for Effective Employee Performance Evaluation in the Banking Sector," *Journal homepage: http://iieta. org/journals/isi*, vol. 26, no. 1, pp. 103-108, 2021.