Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2020 SCPE. Volume 21, Issues 3, pp. 515–541, DOI 10.12694:/scpe.v21i3.1782

SECURITY CHALLENGES IN FOG AND IOT, BLOCKCHAIN TECHNOLOGY AND CELL TREE SOLUTIONS: A REVIEW

NEELAM SALEEM KHAN* AND MOHAMMAD AHSAN CHISHTI†

Abstract. As the IoT is moving out of its early stages, it is emerging as an area of future internet. The evolving communication paradigm among cloud servers, Fog nodes and IoT devices are establishing a multilevel communication infrastructure. Fog provides a platform for IoT along with other services like networking, storage and computing. With the tremendous expansion of IoT, security threats also arise. These security hazards cannot be addressed by mere dependence on cloud model. In this paper we present an overview of security landscape of Fog computing, challenges, and, existing solutions. We outline major authentication issues in IoT, map their existing solutions and further tabulate Fog and IoT security loopholes. Furthermore this paper presents Blockchain, a decentralized distributed technology as one of the solutions for authentication issues in IoT. We tried to discuss the strength of Blockchain technology, work done in this field, its adoption in COVID-19 fight and tabulate various challenges in Blockchain technology. At last we present the Cell Tree architecture as another solution to address some of the security issues in IoT, outlined its advantages over Blockchain technology and tabulated some future course to stir some attempts in this area.

Key words: Cyber Physical Systems (CPS), Internet of Things (IoT), Certification Authority (CA), Public Key Infrastructure (PKI), End user (EU), Attribute Based Encryption (ABE)

AMS subject classifications. 68M10, 68M14

1. Introduction.

While trying to meet our requirements and provide ease and add value in our daily routine activities devices are becoming more ubiquitous. All the devices like those used in industrial automation, households, and smart city framework are now interlinked with the web. From the way we make purchases to the way we drive and even how we get energy for our houses, the IoT is changing much about the world we are living in. As IoT is advancing with time, Cyber-physical System (CPS), mobile internet, several objects, like machines, people, and things are linked into an information zone anytime in any place [7]. Sensors and Sophisticated chips that transmit valuable data are implanted in the physical things that encompass us. A common IoT things platform brings us varied information together and brings the common language for devices and applications to communicate with one another. To decrease latency between the data generation and data processing stage due to the increase in smart applications and requirements, Cisco composed a new term called the Fog computing. Fog computing facilitates smart applications to carry out their action on network devices which can be switches, routers, or gateways, in place of sending data to Cloud datacentres [8]. To aid efficient data access, networking, computation, and storage and to scale the Cloud to the network edge, Fog computing becomes a new paradigm of distributed computing. Fog computing empowers a new variety of services at the edge and also offers a wide range of applications for IoT devices. It also backs heterogeneity, mobility, location awareness, low latency, huge scalability, and geo-distribution. In brief, the objectives of the Fog computing mode are to curtail the data volume and traffic to Cloud servers, improve the quality of service (QoS), and decrease latency [9]. The three-tier architecture is one of the fundamental and generally used architectures in Fog computing as illustrated in Fig. 1.1. The tiers are discussed as follows [10]

- Tier 1–Tier 1 contains IoT- devices, EU's smart hand-held devices (e.g., smart-watches, smartphones and, tablets), sensor nodes, etc. Often, these devices are called Terminal Nodes (TNs) and it is presumed that these TNs are rigged with Global Positioning System.
- Tier 2–Fog:In this layer, the Fog nodes consist of network devices like routers, gateways, switches, and Access Points (APs). Collaboratively, these Fog nodes get to share their computing facilities and

*Department of Computer Science & Engineering, NIT Srinagar, J&K, India (neelam_02phd17@nitsri.net).
†Department of Computer Science & Engineering, NIT Srinagar, J&K, India (ahsan@nitsri.net).

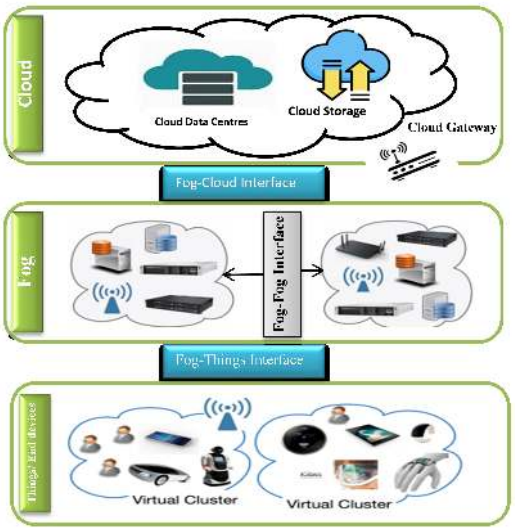

FIG. 1.1. *Three-tier Fog computing architecture [10].*

storage. The fog computing layer is another name given to Tier 2.

- Tier 3–Cloud: The upper layer, Tier 3 is the layer wherein the conventional Cloud servers and Cloud Data Centres (DC) reside. This tier holds adequate resources for storage and computation.

It's imminent that various security and privacy issues will endure sustaining because Fog is a nontrivial extension of the Cloud. While certain existent solutions in Cloud computing could solve many challenges of security and privacy in Fog computing as well, but because of mobility support which is a significant feature in Fog computing, it is likely to present many new security and privacy challenges. These introduced challenges may hamper the adaptability of Fog computing into the IoT. The domain of security and privacy challenges of Fog computing in IoT is yet in its infancy and is open for research.The main motivation behind IoT is to make human lives better and thriving, either by helping people make better choices and live better lives (less pressure, better well-being for impaired individuals, less repetitive jobs), or by making decisions within the framework that positively affect society, the environment, and the economy [1]. Plenty of security loopholes and conspicuous issues came into light after recent attacks on IoT gadgets and these hazards need to be addressed. Overall IoT Security expenditure is approximately expected to reach around $3.1 billion in 2021 estimated by Gartner. Irrespective of the consistent year-over-year increase in worldwide expenditure on IoT security, Gartner predicts that the largest obstruction to its growth will come from a lack of prioritization and implementation of security best practices and tools in IoT initiative planning. This will result in the decline of IoT security spending by 80 percent [2]. As securing IoT has always been in debates and news it becomes apparent that there is a requirement for more secure means of communication. Privacy and security risks were not concentrated to straightforwardly address the necessities of Fog computing. A few investigations were made concerning machine-to-machine communications [4] and smart grids [3]. As Fog devices commission at the Edge of networks on a bigger and more extensive scale, existing Cloud computing security solutions are not sufficient for Fog computing. The habitat of Fog devices is confronted with numerous threats which are not present in the well-governed Cloud [5] In Edge computing, some of the storage and computation tasks are shifted from Cloud data centers to the edge of the network, which might raise several issues related to security and privacy concerns. Specifically, privacy protection and data security are the most vital services in edge computing, which is our significant concern [6]. Individual information collected by IoT devices causes a privacy risk if not taken care of appropriately. So securing the Internet of Things is of utmost significance. Management of the devices should likewise require efficient authentication to abstain from hijacking and botnet proliferation. Therefore, for safeguarding the user and the business data that are collected by IoT devices,

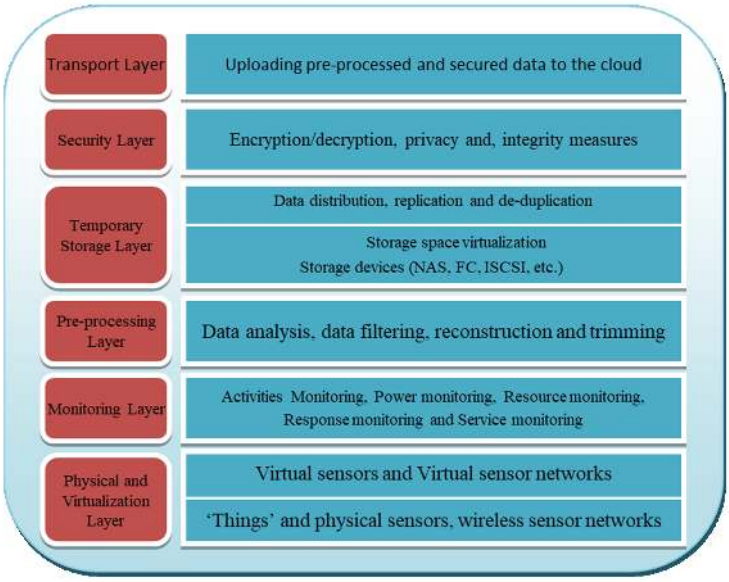

FIG. 2.1. *Smart Gateway-Layered architecture [18]*

innovations ought to be designed with security in mind. With layers of security deployed, overall a 'defense in depth' approach is required. The rest of this paper is divided into four sections. Section 2 provides an insight of various security issues and challenges in Fog and IoT environments. Section 3, then presents the Blockchain, a decentralized technology as one of the solutions, discusses work done in this field and highlights various challenges in Blockchain Technology as well. Section 4, discusses Cell Tree, a novel architecture for storage systems as another solution and highlights its advantages over Blockchain Technology. In lieu of a conclusion, Section 5 offers an outlook towards future development.

2. Related Work. Mohammad Aazam et. al. [18] identified Smart-Gateway-based communication, with Fog computing, the main motive for the design of this framework is for smart communication and aid in reducing the weight on Cloud. It also serves to mitigate the communication burden for the core network. For delay-sensitive applications in Fog computing, the above approach makes normal communication possible in real-time. Also, this technology will make it uncomplicated for the Cloud to create good services more aptly. This perception of IoT, Fog computing, and smart communication with Smart Gateway will bring a great deal of services. Figure 2.1 depicts their concept.

Maged Hamada Ibrahim et. al. [5] in their paper identified an efficient and secure framework that within the jurisdiction of Cloud service provider allows any Fog user in any node to mutually authenticate with any other Fog Server. Their design does not need a Fog user to be assimilated in any (Public Key Infrastructure) PKI. During the registration phase, the Fog user is needed to store a master secret key only once. The Fog server that is controlled by the Cloud service provider will mutually authenticate Fog users using this master key. The protocol comprises three stages: (a) Initialization phase, (b) Registration phase, and (c) Authentication phase.

If any of the Fog servers are compromised and depraved by an attacker, their scheme provides simple countermeasures. The master secret key with large enough bit-length of the client/user stays secure against a brute force even if all the Fog servers are compromised, and therefore, there is no need for the Fog user for any re-registration or re-initialization of a new master key. Also, once a Fog user registers, he is capable of mutual authentication with any Fog server that joins a Fog without the requirement for the user to re-register and there is no extra overhead on the user's side. However, this framework doesn't protect user's anonymity and that is a major drawback. The identity of the Fog user is flagrantly transmitted publicly, in the mutual authentication phase.

To enhance the effectiveness and competency of certificate revocation distribution in IoT surroundings, Arwa Alrawais, et. al. [15] describes a scheme in Fog computing. Their scheme comprises of Fog nodes, a Certification Authority (CA), IoT devices, and a back-end cloud. The proposed scheme offers an efficient certificate revocation information distribution approach. They used a bloom filter to create a shortlist that can adequately curtail the revocation list size with bearable overhead. Their design is a state-of-the-art technique in which all the renounced certificates are delivered immediately from the CAs to the Cloud, and after that to the Fog computing devices. The security of the certificate validation process is ensured by a quick update of the revocation information and it also wipes out the danger of obtaining a revoked certificate. Another way to add to security is to present a proof of reliability by allowing Fog nodes to sign each bloom filter. The signature serves as a definite proof that the vector originates from the Fog, as fabricating or modifying this signature is quite unfeasible. In their framework, the significance of employing the bloom filter is in the reduction of the computational overhead on resource-constrained IoT devices as the bloom filters utilize an effective hashing procedure for the verification of certification status. In this work, the authors also have put forward some possible suggestions for enhancing Privacy, Authentication, Access Control, Location Verification, and so on that still need attention.

In research conducted by Amandeep Singh Sohal et. al. [19], the authors illustrate a Cyber-security technique for diagnosing malignant edge-devices in a distributed Fog computing setting. For the early prognosis of the misbehaving edge devices and reliable edge devices, the proposed framework employs the two-state Markov model and categorizes the edge devices into four classes: Legitimate Device (LD), Hacked Device (HD), Under-attack Device (UD) and Sensitive Device (SD). The edge devices that the Intrusion Detection System (IDS) predicts to be hacked and posting wrong data continuously to the system are the HDs. These HDs although kept alive, are switched to Virtual Honeypot Device (VHD) to predict the path of the attacker successfully. Fig.2.2 illustrates the basic architecture of the Cyber-security framework under consideration which determines the malignant edge devices thereby building a more adaptive Fog computing security system. The main point in the proposed scheme is to allow for a legal edge device to revert from the VHD that may occur erroneously. Also, services to reinforce IDS, adaptive nature and false alarm controller have been included and properly tested. Designing an effective framework that efficiently deals with hacked devices transferred to VHD is a prospective research domain.

For the integrated Edge-Fog-Cloud network framework, Arij Ben Amor et. al. [20] put forth an anonymous and effective communication design. Their work contributes to the establishment of the Fog user-Fog server unidentified mutual authentication design in which the authentication takes place between Fog-server at the Fog layer and the Fog-user at the Edge by establishing a session key with each other without revealing the users' true identity. Whenever a Fog user moves within the same Fog from one Fog server to another, a light weighted authentication is guaranteed. Without the involvement of the Authentication server, the movement from one Fog server to another is done. In Fog-based Cloud computing, a new and secure authentication framework is presented. They conducted the formal validation and security analysis with the AVISPA tool that shows their results have enhanced privacy and security protection in comparison with some current schemes.

Pengfei Hu et. al. [12] in their survey paper discussed various attributes of Fog computing that includes Save bandwidth, Low latency and Support for mobility, Real-time interactions, Geographical distribution, and Decentralized data analytics, Heterogeneity, Privacy Protection, and Data Security, Interoperability and Low energy consumption. Several application cases like gaming and brain-machine interface, health care, augmented reality, IoT, and smart environments are enlisted to illustrate Fog computing applications. The primary technologies, like storage technologies and communication, computing, resource management, naming, privacy protection, and security were also outlined to inform how to reinforce its implementation and application in an elaborated pattern. Finally, some open issues and challenges which are worth farther investigation and research, including privacy and security, energy consumption, programming platform, are laid out. The security and privacy issues highlighted by this paper are explored in Table 2.1.

Saad Khan et. al. [11] in a study reviewed and analysed real-world Fog computing applications to analyse their potential security defects. To give a comprehensive survey, Fog related technologies like Cloudlets and Edge computing are also examined. Most of the Fog applications concentrate on functionality rather than considering security as part of their system, due to which many Fog platforms are being vulnerable. To

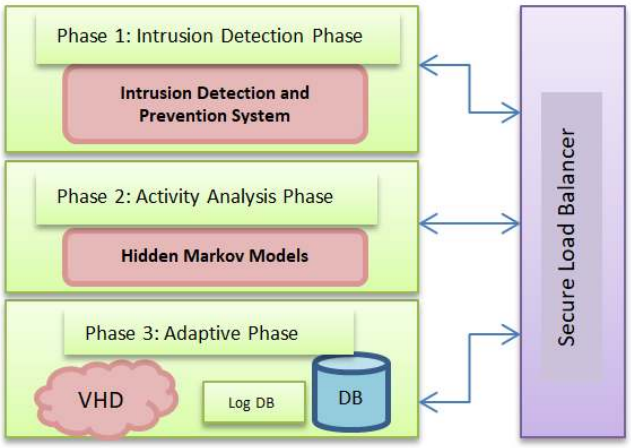

FIG. 2.2. *Three Phase of Proposed Cyber-security Framework [19].*

formulate a systematic review, their study considers following twelve security categories: Advance Persistent Threats (APT), Data Breaches (DB), Access Control Issues (ACI), System and Application Vulnerabilities (SAV), Account Hijacking (AH), Denial of Service (DoS), Insecure APIs (IA), Data Loss (DL), Malicious Insider (MI), Insufficient Due Diligence (IDD), Shared Technology Issues (STI) and Abuse and Nefarious Use (ANU). This paper outlines the examination of how endorsed security solutions might be able to detect, prevent, and proactively shield against the threats highlighted by their survey. The objective of these security solutions is to safeguard the Integrity, Confidentiality, and Availability of the full Fog system and its users. Therefore, the adoption of a decision support system that is competent in saving the Fog platform from potential damage by recommending security measures to developers to prohibit the occurrence of susceptibilities pro-actively.

Eva Marín-Tordera et. al. [21] in their paper first reviewed the up-to-date technologies for Fog computing, paying more concentration to the contributions that inspect the performance edge devices play in developing a Fog node. They concentrated on the core services of a Fog node coupled with the challenges and opportunities towards their practical recognition soon. They present how a conceptual framework is developing towards a consolidated Fog node definition by plotting and comparing the ideas, lessons learned from their execution. After that, this paper also presented a logical view and an architectural approach for the first time about what a Fog node maybe? They categorize the job of Fog computing edge-devices into three fundamental types: 1) "dumb" devices as data producers/consumers, 2) "smart" edge devices with the ability to operate on their data, and 3) "truly smart" edge devices to execute distributed applications. Finally, this paper discusses open issues and challenges that include security and privacy in a Fog-based hierarchical scenario originating when the Fog node must offer a virtualized and abstracted view of its physical resources (i.e., sensing, networking, and computing) to upper layers.

Jun Zhou et. al. [16] identifies various privacy and security challenges in Cloud-Based IoT, recommend some methods to deal with the issues, and highlight future directions for the same. Table 2.2 concludes their paper.

Shahid Raza et. al. [22] has designed a scheme called SecureSense that appends security at the core of Cloud-connected IoT. Amidst a Cloud platform and an IoT device, SecureSense offers secure E2E data communication directly by using standardized Internet protocols. They enabled all three security methods of CoAP by incorporated the security protocol DTLS and IoT protocol CoAP into the SicsthSense Cloud platform and also outfitted these protocols in 6LoWPAN networks. The evaluation shows that the majority of the overall time is taken by the ECC functions and the computation of the Master Secret. The total time is much shorter in Pre-Shared Key (PSK) security mode since neither ECC functions are vital nor all handshake messages are required. These results also conclude that in comparison with the PSK mode, the extra and huge handshake

TABLE 2.1
Summary of Issues, Causes and Challenges in Fog.

Issue	Cause	Challenge
Man In The Middle Attack	Fog devices generally cannot utilize secure communication protocols because of their dearth of resources. Therefore an attacker can eavesdrop or impede the packets between Fog nodes.	The definite solution to Man-In-The-Middle Attack still an open challenge as it has been affirmed to be a silent attack against Fog computing.
Authentication	Entrusting on the Cloud central authentication servers is not a desirable decision, as Fog devices such as gateways may deal with many trust and authentication challenges that were not present in the Cloud case.	A holistic solution should be implemented to establish authentication and trust in the Fog.
Distributed Denial of Service (DDoS)	It is extremely hard for Fog nodes to deal with several requests simultaneously as they are resource-constrained. For a significant period, Fog nodes may become busy, by hurling a lot of insignificant service requests concurrently. With the result, resources that are used for hosting legal services become inaccessible. On the contrarily, Fog nodes can be utilized to eject a DDOS attack.	Compared to traditional DDoS, DDoS attacks using Fog devices will be more serious, the matter of DDoS requires to be addressed effectively in any subsequent Fog computing standardization.
Access Control	In Fog computing, scheming access control to traverse Client-Fog-Cloud and to reach the objectives and resource constraints at various levels is an issue of concern.	To create more powerful Access control mechanisms work needs to be done. The main aim of these techniques should be to help secure association and interoperability among heterogeneous resources in the Fog environment.
Fault Tolerance	There is an immense number of Fog nodes distributed widely geographically; when the service in an area is irregular, users should be able to turn to other adjacent nodes quickly by the alike mechanism.	When there is a breakdown in individual sensors, networks, applications, and service platforms, Fog computing should be capable of providing services normally.

messages for a certificate-based method do not fundamentally devote to the lengthy handshake time. Their outcomes fixed the performance criterion for all the three security methods of CoAP and present that for the Cloud-connected IoT, SecureSense is a feasible E2E communication security answer, in terms of time, storage, and energy overhead. They concluded that it is viable in battery-powered IoT gadgets (having just 32K of RAM) to use the strong government-grade certificate-based security, and the energy and timing overhead is agreeable for most IoT applications.

In another research paper, Antonio Escobar et. al. [23] presented possible ways for combining Cloud computing, Fog, and edge to advocate Internet of Things (IoT) solutions in achieving the challenging IoT needs. Their research concentrated on vertical distribution with clusters and without clusters, as well as sessions and incremental approaches. This paper also highlights that the critical part of IoT communication is Privacy and Communication challenges. It discusses communication with the Cloud using two paradigms viz End-to-Cloud and Gateway-to-Cloud. Drawbacks of both schemes make it crucial to research innovative ways like Transparent Gateways, Hardware Security, and End-to-End Encryption.

The core features discussed by Bidyut Mukherjee et. al. [24] in their paper are: 1) Intermittent Security using Session Resumption concept and 2) Flexible security build on the application resource-awareness. In their paper, they designed an End-to-End IoT Security Middleware. Amidst devices at the network edge and the core Cloud side of an application system lies this Middleware. This Middleware lies between the core Cloud side of an application system and devices at the network edge. This Middleware architecture based on an innovative security design offers affability for securing IoT-based application data, and to help in conditions of unstable network conditions within Cloud-Fog communication platforms by offering immediate re-connections. Their outcomes show the requirement for adaptability in the decision of an IoT security framework depending on resource constraints in bandwidth, computation, network reliability, memory, including the application for which the IoT system is being framed.

Mithun Mukherjee et. al. [9] discuss Privacy and security issues in Fog Computing which includes Trust, secure communication, authentication in Fog Computing, End-user Privacy, and malignant Attacks. This paper summarizes the up-to-date challenges in the domain of Security and Privacy threats for Fog Computing. Finally, they presented some open questions and challenges that can outline a blueprint for future research to resolve

TABLE 2.2
Summary of the issues in IoT discussed by [16]

Issue	Contribution	Future Direction
Fine-Grained Ciphertext Access Control	In Location Based Service (LBS) Fine-grained cipher text access control is a problem. It is seen that this issue can also be unfolded into several dimension scenarios and acquires several applications in outer space security.	A promising solution to this challenge is provided by designing a lightweight attribute-based encryption (ABE).
Location Privacy and Query Privacy	The query privacy would reveal their secret favorites, and moving route disclosure would disclose IoT users' living habits.	Scheming policy-hidden ABE exploiting the approach of a non-interactive proof system for bilinear groups would give us a favorable answer.
Secure Data Aggregation	One-way trapdoor permutation was solely used for secure data collection from a single user in the proposed efficient privacy-preserving technique. It is requisite to expand this proposed efficient privacy-preserving scheme to prevent privacy and security issues in further kinds of Cloud-based IoT. E.g., in smart grid IoT.	To attain secure data collection from multiple users in various types of Cloud-based IoT, a novel efficient privacy-preserving scheme needs to be designed.
Privacy-Preserving Outsourced Data Mining	It is vital to safeguard the user's identity, ensure the accuracy of an outsourced mining solution, privacy and location privacy, and guarantee that the solution can only be accessed by legal entities for example in vehicular IoT.	A challenging open problem is to develop a guaranteed outsourced data mining in the cipher text-domain.
Designing Lightweight Fully Homomorphic Encryption (FHE)	Public Key Fully Homomorphic Encryption (FHE) assuredly presents a substitute to established secure outsourced computation complying both multiplication and addition operations in the cipher text domain. A thorough search of the relevant literature yielded, that the vast volume of computational complexity still considerably disrupts developing lightweight FHE with its numerous application on resource-constrained users in Cloud-based IoT.	An effective privacy-preserving data aggregation without Public Key Homomorphic Encryption will help in the growth of Cloud-based IoT.

various issues in privacy and security in the Fog computing. Table 2.3 summarizes the Fog privacy and security issues that are open to research.

In this article, Yunguo Guan et. al. [26] have summarized the main challenges in solving data privacy and security challenges in Fog computing and identified various apprehensions about why the data security methods in Cloud computing cannot be legitimately adapted in Fog computing. Table 2.4 summarizes Privacy and Security needs in Fog computing as discussed in this article.

Ali Mohammad Saghiri et. al. [27] in their paper proposed a scheme for the Internet of Things based on Blockchain technology and cognitive systems. In their scheme, the status of things (from the things management layer) is detected by the cognitive engine of the cognitive process layer. Later, a convenient index of the smart contracts is triggered by the cognitive engine when it operates on actuators of the things. In the proposed framework, using peer-to-peer communication protocols several crypto currencies (coins) can be used for the payment process. For future research, the technologies of the Web of Things can be applied in the suggested scheme.

In another paper, Mohammad Alshehri et. al. [17] has suggested a new centralized Trust Management scheme for IoT. For the IoT Trust Management scheme, the most important characteristic of their scheme is the Super Node (SN), which is the main trust manager. They have explored the Trust Management Module, API module, and Repository and Communication Module. They have illustrated how it is managed, and how the design works effectively to incorporate trust in IoT communication. Khaled Salah et. al. [29] classifies IoT security issues in three types: Low-level security issues, Intermediate level, and High-level issues as mentioned in Fig.2.3.

Any two parties communicating with each other require authentication between them, to secure communication in IoT. The devices must be authenticated for particular access to services. There are a variety of authentication schemes for IoT. These schemes have distinct heterogeneous underlying architectures and environments which back IoT devices. Thus defining a standard authentication mechanism is a challenge. Also to provide access rights and information to the authorized ones, the authorization mechanism is required.

Syed Rameem Zahra and Mohammad Ahsan Chishti [128] in their paper tabulated the comparison of

TABLE 2.3
Open Research Challenges in Fog Privacy and Security

Issue	Open questions and Research challenges
Trust	In a FogNet, trust relations must be built by the Fog nodes with the devices using Fog network services. Additionally, Fog nodes that are deligated with data and processing requests by the IoT devices are required to create reliable interactions with the Fog nodes. In FogNet this two-way challenge makes the development of the trust model an important task.
Privacy Preservation	To support context-aware service location, the resources of End User's (EU's) devices are shared between other topographically neighboring devices, a large volume of data and other information about the EU need to be ensured in a highly secure manner. In this platform, Sensitive information such as identity and location of the Fog nodes can be easily revealed due to Man-In-The-Middle (MITM) attack. Therefore, to implement identity and location privacy for Fog computing is a formidable concern.
Authentication and Key Agreement	For data aggregated from resource-constrained devices, Fog nodes act as control and data aggregation points, therefore the issue of Authentication is one of the significant worries in Fog computing given the several level of gateways. Hence, Major challenges for Fog computing-based radio access Networks (F-RANs) are the authentication and key agreement protocols and they ought to be explored in the future. Also, to aid fine-grained access control, user-level key management and update mechanisms in a Fog storage framework is a very crucial task.
Intrusion Detection Systems	There is a need to deploy an edge Intrusion Detection System that can integrate the distinct detection components that will be dispersed inside the Fog network [25].
Dynamic Join and Leave Fog Node	A scheme should be designed to authenticate the EUs to the new Fog node and the privacy of the EUs must be preserved whenever a Fog node wants to exit the Fog layer. The errand is to frame a low complexity-based authentication between Fog node and EU is a crucial task in the expandable Fog network. The system should be able to find the users with their real identity once user misconduct is recognized by the Cloud service provider. Also to preserve the anonymity of the users is important.
Cross-Border Issue and Fog Forensic	To knock off cross-border legislation issues in Fog computing is an essential task

TABLE 2.4
Privacy and security requirements in Fog computing [26]

Data services	Different from Cloud computing	Privacy and security requirements
Storage	When processing is completed by the Fog layer, the data content will be altered and unrecognized to the data owner.	• Integrity verification • Public auditing • Minimum overhead • Dynamic support
Sharing	After the Fog layer processes the data, Access control of the data will be altered.	• Authorization revocation • Access efficiency • Fine-grained access control
Query	After the Fog layer processes the data, the keywords of the data will be altered.	• Secure searchability • Refined result • Dynamics support
Computation	The association among the data and computing functions will be altered after the Fog layer processes the data.	• Verifiability of outputs • Confidentiality of inputs • outputs and computing tasks

WSN's and IoT features. Their review also highlights various IoT applications and their security challenges like Smart city, Smart health, Smart building, Smart transport and Smart industry. They concluded that in order to address security issues in IoT environment, WSN's or other ad-hoc networks would not be 100% effective. Therefore more practical and efficient solutions are needed to address these security issues.

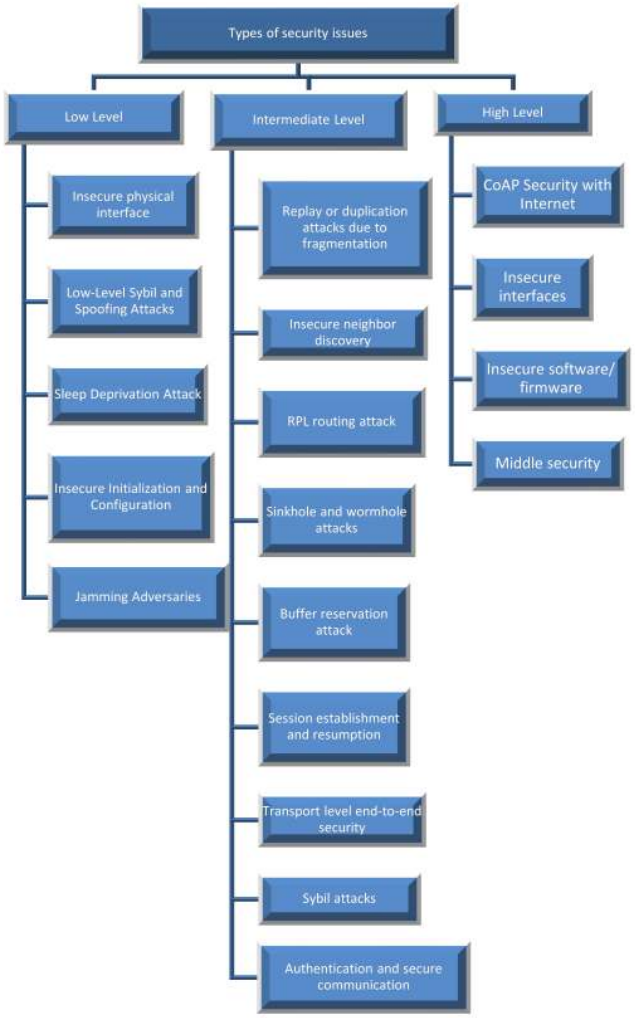

FIG. 2.3. *Three categories of security issues [29].*

2.1. Authentication Issues in IoT. This paper highlights several authentication issues in IoT and their proposed countermeasures by different researchers.

I Authentication and Secure Communication

Implications:

a Using Key Management Systems users and devices in IoT need to be authenticated.
b Any weak opening in security design or huge burden of communication security may disclose the network to many vulnerabilities [30][31][32].
c The overhead of Datagram Transport Layer Security (DTLS) needs to be reduced, due to constrained devices.
d To ensure security, cryptographic techniques are used. These mechanisms must take into account scarcity as well as the efficiency of other resources [33][34].

Proposed Solutions:

1 Compressed AH[42] and ESP[43]

2 SHA1 [92] algorithm takes less time and energy among different encryption techniques
3 Compressed IPsec for an end to end search by Raza [31, 44, 45]. Authors used AH and ESP or providing security using IPsec
4 Distinct versions of SHA1 and AES are implemented by [46] for encryption and authentication.
5 TPM(Trusted Platform module) using RSA [47, 48, 49]
6 Authentication with fuzzy extractor [50]
7 The proposed design by authors in Henze et. al. [52] allows for the configuration of IoT networks from a central location, thus safeguarding the IoT network from distrustful cloud services providers.
8 An authentication scheme that has secure packet forwarding, designed at offering privacy for location and identity on cloud-based IoT is given by Zhou et. al. [53].
9 To secure data communication between IoT devices, a platform in the SMARTIE project by Bohli et. al. [54].

II Transport level end-to-end security

Implications:

a Its main goal is to devise a secure scheme that ensures the correct destination node recieves data from the sender node reliably [35, 36].
b To establish message communication in a cryptographically secure form without disrupting privacy and maintaining the least overhead, a comprehensive authentication mechanism is required [37, **?**, 38].

Proposed Solutions:

1 Brachmann et. al. [35] suggested TLS-PSK , for end-to-end security, while accomplishing communication between HTTP and CoAP.
2 To allow negotiation of session keys, an extension of DTLS with nonce and PSK has been proposed.
3 For TLS, using the 6LOWPAN border router (6LBR) a designated authentication scheme is proposed by Granjal et. al. [36], which precludes the packets, operates on it to execute for the public key authentication computation, and then forwards packets .
4 For 6LoWPAN in tunnel and transport modes, the authors in [30] performed a preliminary assessment of the use of AH and ESP compression header security utilizing AES/CCM encryption at the hardware layer and an assumed application security profile.
5 An architecture coined BlinkToSCoAP for implementing end-to-end security in IoT is proposed in [37].
6 An approach implementing header compression for the 6LOWPAN protocol for decreasing DTLS overhead is suggested by Sinthan et al. [34] and Raza et al. [51].
7 Various header compression schemes have been suggested for implementing Transport Level end-to-end security [56].
8 An improved version of DTLS integrating header compression is suggested in Chavan et. al. [55] for securing IoT.
9 A lightweight design of Internet Key Exchange (IKE) designed to reform key management for 6LowPAN is suggested by Shahid et. al. [38].

III Insecure Neighbor Discovery

Implications:

a In IoT architecture, every device needs to be identified solely. To ensure this, message communication takes place that needs to be secure to assure that data transmitted in end-to-end communication (to a device) reaches the proper destination.
b Before data transmission, the neighbor discovery phase performs various steps along with router discovery and address resolution [39].
c Neighbor Discovery packets may have serious consequences without proper verification usage, along with denial-of-service [29].

Proposed Solutions:

1 Raza et al. [39] propose a security scheme with modules for key generation, authentication, data encryption, and secure neighbor discovery.

2 ECC is used to secure neighbor discovery [57].

IV Middleware Security

Implications:

a The IoT middleware developed to exchange communication between heterogeneous entities of the IoT architecture must be very secure for the provision of services [29] .

b To provide secure communication among heterogeneous entities distinct environments and interfaces using middleware are required to be implemented [40][41].

Proposed Solutions:

1 To secure distributed applications operating in an IoT environment, the VIRTUS middleware proposed by Conzon [40] implements encryption and authentication.

2 A semantic framework called Otsopack [58] works as middleware and uses TSC (Triple Space Computing) for interaction between applications and an open-ID based security method for secure data exchange.

3 Communication between heterogeneous IoT environments is proposed to be supported by a middleware server that has data filtering capability [41].

4 A standard framework with distinctive layers of security is suggested for M2M communication in IoT [60].

5 Open authentication and End-to-end security approaches are implemented in another middleware suggested by Ferreira et al. [59].

V Tampering and Malicious Code Injection

Implications:

a An attacker may physically modify an IoT device or communication link. This is called Tampering [104].

b An attacker can compromise a physical device and inject malicious code Injection onto it [105].

Proposed Solutions:

1 A mutual authentication protocol that is depends upon Physically Unclonable Fucntion (PUF). Depending upon the physical microstructure of device, the authentication takes place using a challenge response mechanism. Thus cloning the exact same structure by altering PUF is impossible which then eliminates tampering as well as malicious code injection [106].

VI Fake Node Injection and Side Channel Attack

Implications:

a In order to control flow of data between two nodes, an attacker can drop a malicious node between two authorized nodes of the network. This attack is called fake node injection [105].

b One of the attacks in side channel attack where in an attacker collects the encryption keys and later uses these keys to encrypt/decrypt data [104].

Proposed Solutions:

1 Aimed for WSN's Porambage et. al. [107] proposed "pervasive authentication protocol" (PAuthKey). PAuthKey obtained certificates from Cluster Head (CH) and then incorporates secure connection among end users and sensor nodes. This scheme successfully eliminates Fake Node Injection. Timing and power analysis attacks cause side channel attack.

2 Inbuilt verifiability of PAuthKey along with physical micro structure eliminates side channel attack [108].

3 A lightweight encryption algorithm along with masking technique can eliminate side channel attack [109].

VII Traffic Analysis, RFID Spoofing and RFID Unauthorized Access

Implications:

a In an attempt to obtain network information, an attacker sniffs the confidential data travelling between IoT devices [104].

b Information is imprinted on the RFID tag [105]. The attacker first gets access to this information by spoofing an RFID signal and then uses the original tag Id, sends its information depicting it as credible. This entire process is called RFID spoofing.

c Data Present on RFID nodes can be read, deleted or modified by the attacker due to absence of authentication schemes leading to RFID authorized access [104].

Proposed Solutions:

1 To protect IoT devices against traffic analysis Liu et. al. Liu et. al. [110] proposed effective and privacy preserving traffic obfuscation (EPIC) mechanism.
2 An on-board SRAM based Physically Unclonable Function (PUF) has been devised by Guin et. al. [111], which generates the device ID; a unique footprint for each IoT device. This ID will reduce the danger of spoofing and unauthorized access.

VIII Routing Information Attack, Selective Forwarding and Sink Hole Attack

Implications:

a In a routing information attack where an attacker creates inconvenience by altering, spoofing routing information, sending error messages, creating routing loops etc [104].
b Selective forwarding is a type of attack where an intruder drops some messages, alters some messages or simply selects some messages and forwards them to other nodes [112]. The result is that destination node receives the incomplete information.
c An attacker attracts other nodes in the network towards a compromised node (known as sinkhole node), so that network traffic flows towards it [105].

Proposed Solutions:

1 For Low power and Lossy Network's a Secure Routing Protocol (SRPL) uses hash chain authentication technique along with rank threshold concept has been proposed by Glissa et. al. [113]. This deals with routing attacks.
2 The above proposed scheme can be used for selective forwarding and sink hole attack. Pu et. al. [114] proposed CMD, a monitor based technique which uses RPL as routing protocol. This helps in detecting forwards misbehaviours.
3 Intrusion detection for SiNkhole attacks over 6Low-PAN for InterneT of ThIngs (INTI) proposed by Cervantes et. al. [115] discloses the identity of the malicious attacker node and isolates the detected sink hole node.

IX Man-in-the-Middle Attack and Replay Attack

Implications:

a In Man-in-the-Middle-Attack (MiTM) an attacker monitors or eavesdrops communication taking place between two IoT devices and gets access to the confidential information [104].
b In reply attack, the network is kept busy by capturing a signed packet and forwarding it over and over again to the destination [112].

Proposed Solutions:

1 MQTT and MQTT_SN suggested by Singh et. al. [116] prevents MiTM attack by ensuring secure device-to- device (D2D) communication. To incorporate Elliptic Curve Cryptography (ECC), MQTT uses Key-Policy (KP) and MQTT_SN uses cipher-text policy (CP) Attribute Based Encryption (ABE).
2 Park et. al. [117] suggested a scheme that prevents MiTM by authenticating inter-device communication. Session keys are generated and distributed by each sensor.
3 Based on Identity Based Cryptography (IBC) Ashibani et. al. [118] has proposed a signcryption scheme. This framework provides confidentiality, authentication and integrity simultaneously and thus prevents replay attacks.

X Data inconsistency, Unauthorized access and Data breach

Implications:

a In IoT, data inconsistency is referred to as the state of data when an attacker attacks on integrity of data during transmission or stored in a database [119].
b In unauthorized access, malicious users can get access to confidential or sensitive data or gain ownership rights [119].

c Leakage of confidential information in an unlawful or unauthorized pattern is called data breach [119].

Proposed Solutions:

1 To secure data transmissions within IoT devices Song et. al. [120] proposed a Chaos-based privacy preserving cryptographic technique along with Message Authentication Code (MAC). This guarantees data integrity.
2 Data stored in remote semi-trusted data storages need to be sure of data integrity, Machado et. al. [121] proposed a three-level split Blockchain based framework.
3 A Blockchain based framework along with ABE has been proposed by Rahulamathavan et. al. [122]. It supports non-repudiation, data integrity, preserves privacy of transaction data, inflicts access control and hence furnishes an end-to-end privacy preserving IoT system.
4 Zheng et al. [123] devices a privacy preserving efficient medical data sharing framework along with ABE.
5 Gope and Sikdar [124] proposed a lightweight privacy preserving two factor authentication schemes for preventing data breach.
6 To reduce the risk of privacy leakage Gai et. al. [125] proposed Dynamic Privacy Protection (DPP) model.
7 The authors in [126] have proposed a protocol called Improved Secure Directed Diffusion (ISDD) for ensuring end-to-end security of data in IoT environments.

2.2. IoT Security Loopholes. Table 2.5 briefly summarizes various loopholes in security of Fog and IoT devices inferred from this literature review which need to be addressed. In-depth analysis of these issues with effective and efficient security techniques need to be developed in order to make IoT a secure platform.

3. Blockchain Technology. Blockchain was devised by Bitcoin [69]. Blockchain extensively offers trustworthy and authorized identity registration, goods, assets, ownership tracking, and product monitoring [67]. Blockchain is the open ledger of all the Bitcoin exchanges that have ever taken place right back to the absolute first transaction. Subsequently the Blockchain is a consistently advancing technology that is continually developing as new blocks are being included. The transactions which are being included onto the Blockchain are being handled by computers associated with the network. These computers are frequently alluded to as nodes. These nodes are situated across the world thus being a decentralized technology. Each block in the Blockchain is appended to the chain in the sequential manner and anything that occurs on the network occurs in general. Blockchain is devised with durability and longevity in mind. It isn't constrained by any single substance. All the hubs that are a part of the network are a part of that community. Consequently it has no single point of failure. There are four key distinguishing features of Blockchain technology listed as follows [96].

1 Use of Smart Contract:Blockchain Technology having no single point of failure and using Smart Contracts, will be feasible to move things of significant worth, for example, property vehicles and so much, more safely. It will forestall any kind of scams that currently exist. This makes it very secure. In this way, smart contracts which when deployed on the Blockchain breathe life into it when purchasing selling, selling-purchasing every one of these things of significant worth. By the pre-eminence of cryptography upon the Blockchain everything will be digitally scanned and digitally signed. It will be a safe and effective method of moving things of profound worth.
2 Peer-to-Peer system: Another distinctive property of the Blockchain technology is that it cuts any kind of agent in the course of action. At the center of this technology is a peer-to-peer framework which is ensured security by cryptography, henceforth it has the ability to pull out attorneys, estate agents, account assistants and different experts from the center of the procedure e.g., when selling a house you can encourage that transaction legitimately through the Blockchain, consequently saving your cash.
3 Speed: Third distinguishing factor of Blockchain technology is that it allows for deals, transactions and all kinds of stuff completed very quickly e.g., the property deeds could be traded very quickly. It soothes out these regularly tedious assignments.
4 Capacity: Due to Peer-to-peer technology capacity of the whole network can be increased.

Blockchain does not only have impact on financial world but also contains other fields. These include digital rights, betting, debt management, escrow transfers, microfinance lenders, equity markets, private markets, the Remittance industry, and crowd funding platforms, derivative markets, land record deeds, E-commerce sites, global payment systems, P2P lending services, healthcare services, ownership records, election, casting a ballot

TABLE 2.5
Loopholes in Fog and IoT security

Loophole	Description	Reference
Cyber Attack	Due to huge quantity of data throughput and the probability of being able to obtain delicate information from both IoT devices and cloud, the Fog platform is a tempting target for Cyber-criminals.	Saad et. al. [11]
Denial-of-Service (DoS) attack	Denial-of-Service (DoS) attack is one of the malicious attacks that can be attempted. As a majority of the devices linked to the network are not mutually authenticated, therefore hurling a DoS attack turns out to be straight forward.	Mithun et.al. [9] Pengfei Hu et. al. [12]
Mobility of Fog nodes	One more important issue is that since Fog nodes leave or join the Fog layer time and again; Fog nodes are very dynamic. The well-studied Security and privacy techniques in Cloud Computing are not precisely applied due to the mobility of nodes.	Mithun et.al. [9]
Authentication	The End User's (EU) randomly moves around over the network and the Fog nodes joins and leaves a Fog layer frequently. Thus, the process of mutually authenticating EU's and Fog node is quite a challenge. To carry out data and processing requests by Fog nodes, EU's need to establish trusted relations with the Fog node. In IoT Authentication witnesses considerable challenges in efficiency and scalability. Traditional authentication methods remain insufficient, and there exists a demand for an efficient, secure, user-friendly and scalable scheme to cater to the needs of resource-constrained IoT devices.	Maged Hamada Ibrahim et. al. [5],Alrawais et. al. [15]
Efficient Intrusion Detection techniques	Currently, Intrusion Detection techniques are commonly utilized to alleviate attacks such as DoS attacks, scanning attacks, insider attacks or Man-in-the-middle attack. By employing IDS methods at each level of Fog Computing, many challenges emerge, such as false alarm control, real-time notification, correct response, and alarm parallelization.	Anwar et. al. [13]
Access Control	In Fog computing, another challenge is Access Control. How the access control policies are designed to traverse client-Fog-Cloud to serve the aims and resource constraints at different levels? The open issues need to be addressed to develop more robust Access Control policies that aim to strengthen interoperability and secure collaboration among the heterogeneous resources in Fog.	Pengfei Hu et. al. [12]
Public Key Infrastructure (PKI)	Managing the Public Key Infrastructure (PKI) which is needed to support secure communications is a significant challenge.	Stojmenovic et. al. [14], Law et. al. [28]
Location Based Service	IoT users living patterns would be exposed by moving route exposure and the query privacy would reveal their private favourites, query privacy and location privacy for Cloud-based IoT users in LBS (Location Based Service) has to be well preserved alongside privacy, trust, and authentication.	Zhou et. al. [16]
Mischievous Nodes	Minimal work has been done until now on the authority of trust or security improvement in the IoT environment, particularly concerning handling with mischievous nodes that are presently legal members of an IoT community.	Mohammad et. al. [17]
Resource Limitations	IoT devices have resource limitations. This requires protocols to be energy-efficient and lightweight in spite of requiring tedious calculations along with the advancement of energy harvesting methods.	Kamalinejad et. al. [64]
Heterogeneous Devices	Multi-layer security technology is required to be incorporated for heterogeneous devices that range from small low power devices with sensors to high-end servers.	Khaled et. al. [29]
Conversion Mechanism	The protocols incorporated at various levels need to interoperate by providing conversion mechanisms, for standardizing a global security mechanism for IoT.	Khaled et. al. [29]
Single Point of failure	The IoT environment is more vulnerable to single points of failures because of heterogeneous networks, protocols, and architectures.	Khaled et. al. [29]
Standard Verification Protocol	A standard verification protocol is an important element for tackling IoT security. Vulnerabilities should be exploited before deployment because after deployment it gets difficult to detect and alleviate. Along with physical malfunctioning, the implementation of a security algorithm in the hardware, packet processing, and routing mechanism also needs to be verified.	Khaled et. al. [29]
Scalable and Trusted Management, and Software Updates	Scalable and trusted management and software updates to millions of IoT devices are one of the open challenges.	Khaled et. al. [29]
User's Anonymity	In most of the research conducted on Fog, user's anonymity has not been protected. Identity of user is transmitted over public channel.	Maged Hamada [5]
Hacked devices	Designing an effective framework that efficiently deals with hacked devices transferred to virtual honeypot devices (VHD) is a prospective research domain.	Amandeep et. al. [19]
Privacy and Communication challenge	The critical part of IoT communication is Privacy and Communication challenge. It is crucial to research innovative ways like Transparent Gateways, Hardware Security, and End-to-End Encryption.	Antonio et. al. [23]
Revision of existing solutions	With the tremendous growth of IoT devices and with new attacks emerging due to changes in economic incentives or discovery of new bugs, the existing solutions may need revision.	Acharya et. al. [83]

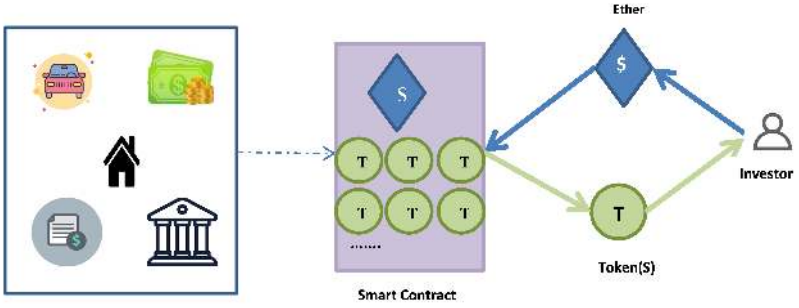

FIG. 3.1. *Ethereum Blockchain.*

and Intellectual property rights.

The Blockchain ensures trustworthy decentralized management, administration, and tracking at each phase in the supply chain and life span of an IoT device. Blockchain assures data integrity and authentication by ensuring that data being transmitted is cryptographically secured and signed by the legitimate sender. Blockchain smart contracts can ensure Authentication, Authentication, and Privacy. Every IoT device once installed and connected to the Blockchain network would have his unique GUID and symmetric key pair; therefore in Blockchain distribution and key management are wiped out completely. This will result in the use of lightweight security protocols. These lightweight protocols would fit and organize the need for the compute and memory resources of IoT devices. Blockchain guarantees tamper-proof storage of authorized transactions. Blockchain is used within IoT to store sensor data, manage device configuration and enable micro-payments [68]. Blockchain technology excludes the requirement for 3rd party verification [71].

3.1. Understanding the strength of Blockchain. The address space of Blockchain has 160 bit as compared to 128 bit in IPV6 [29] . Address length is 20 bytes or a public key generated ECDSA hash of 160 bit. Ethereum Blockchain was created with decentralized applications in mind [97]. Ethereum is launched in 2015 by Vitalik Bulterin. It is the world's programmable Blockchain. Ethereum laid the beginning of a new era of internet where i) payments and money are inbuilt ii) clients can own their data and apps cannot steal from you or spy on you iii) an open financial system becomes accessible to everyone iv) no person or company is the controller and is built on neutral, open access infrastructure. The 'ether' is the crypto currency that powers the Ethereum. Fig.3.1 illustrates the working of Ethereum Blockchain.

The Ethereum transaction has a couple of parameters as shown in the Fig. 3.2. The basic set of steps in realizing the strength of Ethereum Blockchain are as follows:

I User sends the Ethereum transaction ***Ti*** from a wallet (say metamask).

II The user has a private key ***Pr*** which is 32 bytes long and is randomized, 64-hex character string. Private keys can be generated at the user end by using a safe randomizer.

III ***Pr*** is sent through a function which is called ***ECDSA*** (Elliptic curve digital signature Algorithm). This function produces public key ***Pk*** which is 64 bytes long. ECDSA has property that ***Pk*** can be created from ***Pr*** but ***Pr*** cannot be created from ***Pk*** (without trying all combinations). This is strength of Blockchain.

IV Create hash of the ***Pk*** by using the ***Keccak-hash(Pk)*** and take last 20 bytes of that i.e., ***B96.....255***. This would be the Ethereum Account (from field of the transaction).

V ***Ti*** is signed by ***Pr***. The output will be signed transaction ***Tis***.

VI ***Tis*** are run through the ***ECRECOVER*** function. The output will be ***Pk*** and the Ethereum Account (from field of the transaction).

This will make sure that the Ethereum transaction is authentic. It can be made sure that the account that was used in the 'from' field of the transaction is the same account that has the underlying private key that was used to sign the transaction and create the transaction signature. This is why in Blockchain every participating node can easily verify if the transaction is correct. The entire procedure is illustrated in Fig. 3.3.

All the blocks are chained together using cryptographic hashing [98]. Each block contains the hash of the

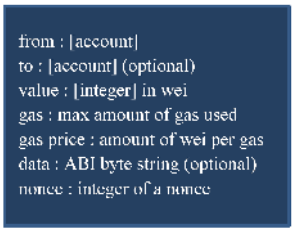

Fig. 3.2. *Ethereum transaction.*

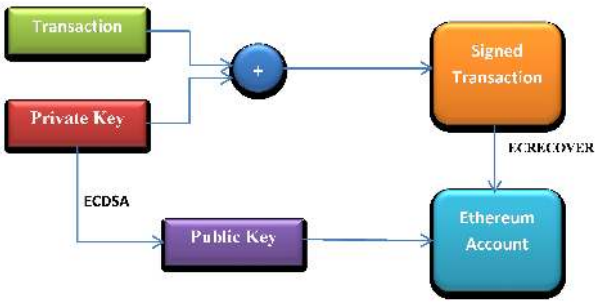

Fig. 3.3. *Understanding strength of Ethereum Blockchain.*

previous block, to ensure the correct sequence of transactions in the Blockchain, as shown in Fig. 3.4 Blocks have hashes of the previous block and this ensures transaction integrity. Any alterations to the transaction(s) in a block will alter all the blocks thereafter. In the event that a hacker attempts to alter any transaction, not only does he need to modify the transaction in the block, but all other blocks in the Blockchain. Moreover, hacker additionally needs to apply the change to every single node on the network, which is a computationally costly job to do. Each Blockchain has its own genesis block, which is the initial block of every Blockchain. The Bitcoin network has its own genesis block, and likewise Ethereum has its own genesis block.

Every participating node in the network has the copy of same information. Full nodes are the computers that store the Blockchain. Fig. 3.5 shows the full nodes in the Blockchain network containing the Blockchain.

Mining. Mining process creates new blocks on the chain using miners. A miner has following tasks:

- Combine the hash of the previous block and its transactions to derive a new hash
- The new hash is stored into the current block

To guarantee that all the miners have an equal opportunity to mine a block, Blockchain network will add a difficulty target in each block. So, result of the hash must meet the difficulty target to mine the block. In order to achieve this, miners inject a number called nonce into the block. Now miners will compete with each other in order to meet the difficulty target by guessing the value of nonce. So, the job of miners basically is to find the value of nonce.

This process of identifying the nonce is called Proof-of-Work (PoW). When the block is mined successfully change is accepted by all the nodes. The key idea behind PoW is that finding a nonce is difficult but verifying a nonce is easy once it is found. When mining is successful, the respective miner earns mining fees as reward.

3.2. Blockchain and IoT related work. Mayra Samaniego et. al. [68] discusses that a hosting location for deployment of Blockchain is a key challenge. Hosting on resource-constrained IoT devices is not advisable due to: a) Absence of computational resources b) Absence of sufficient bandwidth c) Need to preserve power. The paper performs experiments for both cloud and fog as a hosting platform. The findings of their evaluation are that Fog outperforms cloud. The fog has low latency while the cloud has high latency. Dr. B. V. Ramana Reddy [93] discusses four components of Blockchain as in Fig. 3.6.

Oscar Novo [70] in his paper brings forth some of the following benefits of access control in IoT as illustrated

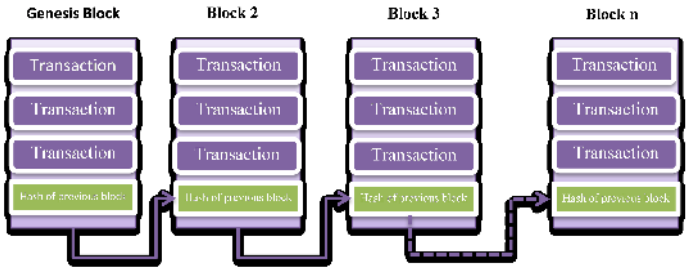

FIG. 3.4. *Hashing to chain the blocks in a Blockchain.*

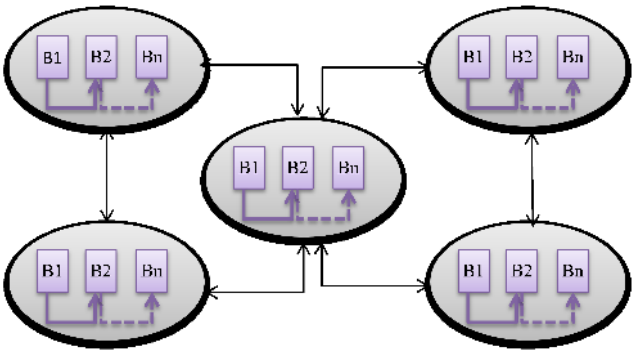

FIG. 3.5. *Nodes in the Blockchain network.*

in Table 3.1. The main focus of this research is on spawning a single smart contract that describes the policy rules of the administrative framework. Also, larger units of IoT devices that are not capable to execute Blockchain technology are included in their framework. The solution this paper provides experiences the burden of wait that the Blockchain network suffers in order to release the access control information. This waiting sceptically influences the performance of the proposed framework. The performance of the management hub is acceptable. The capability of IoT devices with respect to scalability is overall acceptable. In the proposed solution various threats as mentioned in Table 3.2 were identified using the STRIDE [72] model. Their research also suggests a solution for these security issues by introducing certification Authority. The CA will sign the management hub nodes and through this process the IoT devices could check the validity of the management hub.

A. Ouaddah et. al. [73] in their paper presented FairAccess as a new decentralized pseudonymous and privacy-preserving authorization management system that uses the steadiness of Blockchain technology to handle access control on account of constrained devices. This FairAccess is a crypto currency Blockchain based access control framework. For every resource-requester pair, their proposed model creates a distinct smart contract for the access control policy.

Nallapaneni Manoj Kumara et. al. [74] in their paper explains the probable security and privacy issues in consideration of the component intercommunication in IoT. The issue in centralized data Management Servers (CDMS) is that more arrangements and possibilities exist for revealing the sensitive parts of the data to the outside world through the false authentication, device spoofing. This paper mentions three major components of IoT as shown in Fig. 3.7 i) Things with Networked sensors and Actuators (TNSA) ii) Raw Information and Processed Data Storage (RI-PDS) iii) Analytical and Computing Engines (ACE). This paper also mentions various challenges faced by the integration of Blockchain technology with IoT that includes Limitation with storage facility, Lacking of skills required in the field, Lack of workforce, Legal issues, Variation in Computing Capabilities, Processing time and Scalability.

The authors in [66] discussed various issues of identity in IoT which included ownership and identity

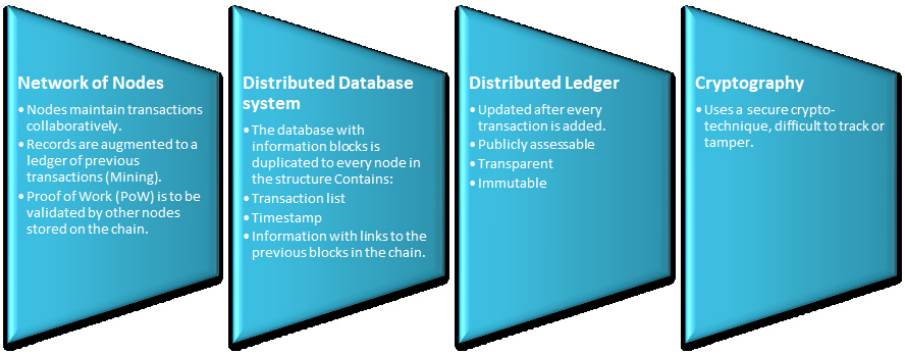

FIG. 3.6. *Four Pillars of Blockchain Technology.*

TABLE 3.1
Advantages of access control in IoT

Advantages	Description
Mobility	To manage IoT devices every administrative domain in the network has freedom of its own. Access control is enforced by rules in Blockchain.
Accessibility	The system allows the accessibility of control rules at any time. Also, all the information regarding access control is distributed; therefore any event of some server failures doesn't prevent access to such vital information.
Concurrency	Multiple managers are concurrently granted access or ability to update the access control protocols.
Lightweight	No modification required to adapt their solution by IoT devices. Through the Blockchain network, communication amongst all the managers and IoT nodes occurs, thereby facilitating cross-platform communication.
Scalability	Supports multiple IoT devices interconnected by the various constrained networks to a single Blockchain.
Transparency	The system conceals the IoT device locations and also in what manner any resource is accessed.

relationships, authorization and authentication, governing of data and privacy. Slock.it [99] developed slock that is a smart lock technology which enables the Blockchain technology to control physical objects like (cars, bikes or houses). TransActive grid developed a technology that is a collaboration of hardware and software. This technology enables users to buy and sell solar energy securely from each other [100].

Based on Blockchain technology, Filament has built an open technology stack that enables devices to communicate, discover, and interact with each other in a completely distributed and autonomous way [100]. Bahga et. al. [61] introduced a decentralized peer-to-peer framework called BPIIOT for Industrial IoT using Blockchain Technology. Without the requirement of a trusted intermediary, the BPIIOT framework permits peers in a trust less network to connect. BPIIOT has an adequately wider scope than Slock.it and is capable of developing various peer-to-peers and distributed manufacturing applications. This paper mentions some benefits of Blockchain for IIoT as listed in Table 3.3.

To support the sharing of services among IoT devices and autonomous workflow, the authors in [62] [63] described smart contracts of the block that can facilitate the above thing. Seyoung Huh et. al. [75] proposed Blockchain to control and configure IoT devices. RSA public-key cryptography is used to manage keys; Ethereum stores the Public keys and on individual devices, the private keys are stored. This paper discusses in their evaluation that it has 12 sec transaction time and for time-sensitive domains, such topology may be difficult. Also to save entire Blockchain a proxy or a huge repository is needed. Utilizing a proxy can be simple but may jeopardize security as a third party is engaged. Another solution would be to utilize a large repository which would be very costly and still not feasible to cater to small IoT devices.

Sayed Hadi Hashemi et. al. [77] defines a complete architecture of three layers having Blockchain at the storage layer. Their work also defines data sharing protocol, data management. This paper also discusses different mechanisms and their impact that includes direct access to Blockchain, Client access, Publisher subscriber access.

Matthias Mettler et. al. [78] discusses the role of Blockchain in healthcare. Blockchain technology offers opportunities for usage in managing public health, drug counterfeiting, medical research that is user-oriented

TABLE 3.2
Threats identified in [70]

Threat	Effect
Spoofing	A noxious management hub could impersonate a management hub
Tamper	Access control information that is directed to the IoT devices can be altered
Repudiate	A device can claim that they have not taken any activity.
DoS	Debase the data directed to an IoT device or unveil unapproved data of the IoT device

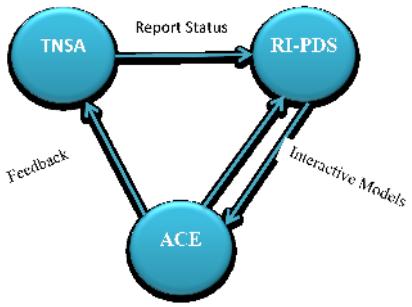

FIG. 3.7. *Three major components of IoT [74].*

and based on private patient data. It will also help advances in the latest digital health and business model initiatives. Asaph Azaria et. al. [79] discussed smart contracts in IoT. Their work describes the application of Blockchain to manage and access medical records, manage the relationship between different parties of Blockchain. They put forth the idea of having a decentralized record management system to manage EMRs (Electronic medical records) by employing Blockchain technology. When handling sensitive information crucial considerations are Confidentiality, accountability, authentication and data sharing. MedRec manages all of them.

Jie Zhang et. al. [80], discuss the use of Blockchain technique in PSN-based (Pervasive Social networking) healthcare. An updated version of the 'IEEE 802.15.6 Display Authentication Association' protocol is developed to initialize secure links.

Zyskind et. al. [81] discussed Blockchain implementation in a cryptographic approach, to protect personal data. This paper proposes a platform that enables Blockchain technology as an access-control moderator having an off-Blockchain storage solution.

Nabil Rifi et al. [76] put forth a Blockchain technology based publisher- subscriber technique and a data access protocol by adopting smart contracts. This paper used the model based on smart contracts that allow authentication, maintaining regulations, and communication among various nodes and groups of the system. The last component of the system uses off-chain database IPFS [82].

Authors in papers [84] [85] have proposed a solution to reduce the content stored on Blockchain, using alternate consensus mechanism [86][87][88] and using different graph topologies [89][90].

Leemon Baird et. al. [89] proposed Hedera a distributed ledger platform as well as an organization that resolves the aspects that restrict public DLT acceptance by the mainstream. A novel platform for providing consensus in a distributed setup is realized through a data structure called hashgraph and consensus algorithm. This paper also highlights the differences between Blockchain and hash graph. The hashgraph performs being quick, fair, ACID-compliant, lo-cost, efficient, time-stamped, Byzantine and DoS immune.

Serguei Popov [90] discussed the tangle that consists of a directed acyclic graph (DAG) for saving transactions is the next evolutionary stride that succeeds in the Blockchain.

Xiaoqi Li et. al. [95] in their paper presented several security issues of Blockchain technology. In their research they discussed every possible risk and vulnerability in Blockchain and also analyzed its probable causes and consequences. Their work also highlighted some real world attacks on Blockchain, and focused on the exploited vulnerabilities that lead to these types of attacks.

TABLE 3.3
Benefits of Blockchain for IIoT

Benefits	Description
Decentralized and Trust less	Each transaction in Blockchain is verified and validated through the consensus between all the transacting peers since it is decentralized; the peers need not to trust each other.
Resilient	Since Blockchain architecture is not centralized, the single point of failure doesn't exit. Blockchain cannot be altered or deleted, so Blockchain is an immutable ledger.
Scalable	As many new peers (or miners) keep on joining the chain, computing capacities of the network scales up.
Secure and Auditable	The security of every transaction on a Blockchain network is guaranteed by secure cryptographic methods and auditability as every transaction is transparent to everyone on the network.
Autonomous	No trusted third party is involved as all the IoT devices perform transactions autonomously with each device owning its Blockchain account.

According to [102], blockchain technology is now evolving as an influential framework for COVID-19 management. Blockchain was a focus to Chinese government since October 2019. After the 2020 corona virus breakout, the Chinese hospitals have been using Blockchain technologies in several applications like electronic heath records to insurance claims. Popular pharmaceutical companies have cooperated with software corporation SAP SE, of Walldorf, Germany, on Blockchain solutions for tracking of supply chain and identification of fake drug identification. As tests are conducted for COVID-19 vaccines and treatments, Blockchain can be used to endorse the trials. Furthermore, Blockchain can be adapted to learning about the monitoring disease outbreak patterns.

The rapid and uncontrolled outbreak of COVID-19 [103], points out the collapse of existing healthcare surveillance systems to manage public health emergencies on time. Blockchain is emerging as a tool to aid with several facets of containing the outbreak. The US department of Health and Human services office of the National coordinator for Health Information Technology broadcasted a nationwide interoperability guidelines requisitioning ubiquitous, secure infrastructure, authenticates all the participating entities, identity verification and persistent representation of authorization to access electronic health information. Blockchain technology could meet these expectations as it is a decentralized architecture, with main aspects like, data provenance, immutable audit trials and robustness. While keeping data privacy and security regulation intact, multiple nodes in permissioned Blockchain share and report important information instantly. Blockchain assists with prevention and control of disease by offering ways to improve many public health activities. The use of Blockchain can assist in prevention of pandemic by enabling early observation of epidemic, faster tracking of drug trials and impact management of outbreak and treatment.

The increasing demand of electronic medical records (EMRs) at this time of COVID-19 panedemic is evident. With security, privacy and transparency benefits of Blockchain, health records on it are eagerly pursued but extremely difficult to do. This time of crisis like COVID-19 will encourage research directions in this field in order to implement this at national and global levels [129].

Jayasree et. al. [127] in their review paper categorizes security attacks in IoT into four broad domains: (a) Physical Attacks (b) Network Attacks (c) Software Attacks (d) Data Attacks; and lists various countermeasures in these categories. Their paper also highlights the evolution of Blockchain technology and its benefits when incorporated with IoT and IIoT. Their survey discussed various security issues in IoT and IIoT w.r.t Blockchain technology and traditional solutions that need to be analyzed in-depth.

3.3. Challenges in Blockchain Technology. Table 3.4 briefly summarizes various issues in Blockchain Technology in IoT inferred from this literature review which needs to be addressed. In-depth analysis of these challenges with effective and efficient techniques needs to be developed in order to make Blockchain and IoT emerge as a promising platform for future.

4. Cell Tree. Cell Tree is a novel architecture for distributed storage systems that facilitates the storage of data in highly programmable and largely independent cells that are "assimilated" into a tree structure. Each cell has its policies and it allows data to change over time. Each cell is governed by its selected crew. The architectural design goal is to allow the evolution of the cell tree organically and designed to adapt itself across several applications. Anasuya Acharya et. al. [83] proposed a distributed data repository. The key philosophy

TABLE 3.4
Challenges in Blockchain Technology

Challenge/Issue	Description	Reference
Storage	All nodes connected in IoT store a replicated ledger on a Blockchain. Therefore, if stored on the Blockchain itself, storage would prove to be quiet inefficient.	Nabil et. al. [76]
Time consuming	The process of mining and validating blocks is time consuming as the count of nodes and the transaction count continues to grow.	Nabil et. al. [76]
Vulnerable	Blockchain provides robust approaches for securing IoT, but the approach is still vulnerable.	Jiang et. al. [65]
Secure Mining	Miners hashing power for the consensus mechanism can be jeopardized, therefore permitting the attacker to host the Blockchain.	Khaled et. al. [29]
Private Keys	Blockchain accounts can be compromised because of the limited randomness of private keys.	Khaled et. al. [29]
Race attack	Race attacks should be avoided which can cause double-spending during some transactions.	Khaled et. al. [29]
Scalability	Blockchain architectures face scalability challenges. All the full nodes are required to store the whole chain in order to fully validate any new blocks as the underlying Blockchain framework is ever-expanding.	Acharya et. al. [83]
Illegal content	The data stored may include illegal content which may result in legal complications for the Blockchain.	RomanMatzutt et. al. [91]
Irreversible effects	Due to the immutable (unable to change) nature of Blockchain, any implementation bugs can create irreversible effects.	Acharya et. al. [83]
Expensive POW	The consensus protocol employed by Blockchains called Proof-of-Work (PoW) ecologically turned out to be expensive. Therefore, this is another Blockchain limitation.	Acharya et. al. [83]
Availability and Consistency	In distributed architecture of data systems, there exists a trade-off between availability and consistency. Blockchain remains available and partition tolerant at the cost of its consistency. In Ethereum, the Blockchain resulted to be considerably faster than the Bitcoin. One major consequence of a quicker block time is its diminished security; therefore for newly mined blocks, multiple confirmations are required by many Blockchain applications to prevent transactions from double-spending.	Bahga et. al. [61]
Software Vulnerabilities in Smart Contracts	Smart contracts may suffer from software vulnerabilities that can be manipulated by hackers.	Bahga et. al. [61]
Risk of Attack	On a Blockchain, smart contracts serve as policy agreements between transacting groups that are not legally enforced to the outside network, any attacks can pose risks to the organisations, block miners and also to the entire Blockchain network.	Siegel et. al. [94]
Lack of Awareness	The lack of knowledge and awareness about the Blockchain technology in domains other than the financial sector, affects its widespread adoption.	Bahga et. al. [61]
Lawful Enforcement	Some regulations for decentralized systems like Blockchain and the need for lawful enforcement of smart contracts are needed in order to mitigate any conflicts among transacting groups.	Bahga et. al. [61]
Blockchain Adoption in Indian healthcare System	Since Blockchain is a decentralized architecture, its servers are across geographical regions. In order to keep transaction data encrypted high computing power is required that consumes lot of electricity which is deficit in India. As of today a uniform IT system for healthcare has not been implemented in India. One of the challenges in adoption of Blockchain is limited insight into the product lifecycle. India does not have prerequisite assets in place to go ahead with digital health system.	Garg [130]

is to allow for different solutions in the single system to coexist so as to facilitate the evolution of the system with time over several applications. The complete framework is agnostic to how every module is implemented, as several sub-problems are assigned to modules. In their design, an important feature is to allow for different users of the system to focus on different parts of the structure and remain burden less by the whole system data. Another thing in their proposed architecture is having a multi-level confirmation for new connecting blocks so that clients that trust the nodes in the lower levels of the hierarchy receive a quick confirmation of any block added to the system, and the ones that don't trust would wait for a confirmation from higher levels. The cell tree framework strives to be modular, cellular and evolving. The basic building block of the cell tree

TABLE 4.1
Comparative analysis of Cell Tree and Blockchain technology

	Blockchain	Cell Tree
Nodes	A conventional Blockchain can be viewed as a single node Cell Tree, with a programmed cell and a large crew.	A Cell Tree has many parallels with Blockchain in lieu of Blocks.
Multi-Level confirmation	In Blockchain framework, the entire chain is bound to accept any system update that takes place.	In a Cell Tree, based on its local policies, a Crew that operates a node updates its cell independently and then assimilates it into the tree.
Reserved Hash Pointers	Blockchain uses chain topology. In this, recently linked nodes bear 'hash pointers' to previous nodes. The reversed direction of hash pointers reflects the fact that in a conventional Blockchain, a block gets confirmed when future blocks attach to it.	Cell Tree uses tree topology. In this, the 'hash pointers' refer from old parent node to its new child nodes. In Cell Tree, a Cell (or an update to a cell) is confirmed by already existing nodes.
Distributed Ownership	In a Blockchain, for each fork, consensus throughout the entire network will be required, if multiple forks have to be essentially retained, making it infeasible as the numbers of forks grow.	In Cell Tree architecture, every single node is claimed and controlled by its own designated crew. The scalability of the framework greatly improves by associating the ownership of nodes to comparably small crews that function in parallel. Regardless of whether a node's crew behaves nefarious, any amends introduced to the node's cell get incorporated into the Cell Tree only after they get verified and acknowledged by the crews supervising it.
Dynamic Nodes	Blockchain focussed on the immutability or 'persistence' assurance of the block.	Cell Tree introduces 'consistency' to guarantee that each cell has been developed into its current form in consistency with the protocols defined by the cell.
Excising Malignant Cells	In Blockchain, the blocks that belong to a chain cannot be removed as per Blockchain design. This may lead to socio-legal issues whenever any unlawful data is facilitated over a Blockchain.	A Cell Tree allows to make deactivation of the malignant cells viable to, with a minimal effect on the complete tree.

TABLE 4.2
Features of Cell Tree

Features	Description
Mirroring, Pruning, and Grafting	Subtrees are allowed to be pruned from or to be grafted on a Cell Tree. In terms of mirroring, grafting is possible in multiple locations with little impact on other nodes.
Excising Cells	If the crews of all the nodes supervising it agree, the contents of a cell can be detected or may be changed without any respect to its program.
Computed Reads	A function of a cells' content can be accessed.
Secret Cells	Through confidential sharing or protected multi-party computation policies, the crew members of a node can offer to legitimate clients access to the contents of the cell or to the functions (crew members need not be aware of cell contents)
Computing or Multiple Cells	Framing of concurrent algorithms to work independently on each cell.
Saplings	A Cell Tree having its root incorporated into some other parent Cell Tree is termed as a sapling.
Higher Arity Trees	By permitting a particular crew to handle a subtree rather than a single node, Higher Arity nodes may be effortlessly simulated.
Incentivization	Different parts of a Cell Tree may employ different incentivization mechanisms.

is a cell that holds the data and an (even smaller) nucleus. Nucleus has code that specifies how a cell can evolve. A cell is hosted as a node of a binary tree. Each node is operated by a crew. The crew of each node is also authoritative to monitor nodes in comparatively small subtree that is rooted there. Several algorithms have been implemented by the crew members that define how cells evolve, policies for monitoring how some other cells evolve, and means to incorporate changes and distribute assimilation information across the tree [83]. Table 4.1 presents a comparative analysis of Cell tree and Blockchain. Cell Tree has several other features highlighted by the paper [83] that can be used to further strengthen the security aspect of IoT as listed in Table 4.2.

5. Conclusion. Currently, the Fog platform is primarily an active point for cyber-crimes due to a lack of centralized control and poorly secured edge nodes. Also, since majority of devices networked together are not being authenticated mutually, attacks become inevitable. Keeping in view the very dynamic nature of Fog nodes that keep on joining or leaving the Fog layer very frequently the current stringent security and privacy policies adapted in Cloud Computing environment are not directly applicable due to node mobility. In this paper we tried to highlight various risks and vulnerabilities in Fog environment and reviews countermeasures in this field. With resource-constrained IoT devices, authentication faces several challenges such as scalability and efficiency. In this review, we tried to highlight several authentication challenges in IoT and outlined existing solutions in this domain. This paper further tabulates security loopholes in Fog and IoT environments. We focused on Blockchain as one of the solutions for authentication in IoT, analysed its strength, reviewed existing research in this field, researched about its adoption in COVID-19 fight and summarized challenges faced by Blockchain technology in IoT environment. Finally, we proposed Cell Tree a novel architecture for storage systems as another solution for eliminating some of security issues in IoT, summarized its advantages over Blockchain technology and tabulates its features which can be implemented to improve the efficiency of IoT security.

REFERENCES

[1] D. Bastos, M. Shackleton and F. El-Moussa, *Internet of Things: A survey of Technologies and security Risks in Smart Home and City Environments* in IEEE Conference on Living in the Internet of Things: Cybersecurity of the IoT, London, UK, 28-29 March 2018.

[2] Gartner, *[2] Worldwide IoT Security Spending Forecast*, https://www.gartner.com/newsroom/id/3291817. (Last accessed on 15 may 2020.

[3] W. Wang and Z. Lu, *Survey Cybersecurity in the smart grid: Survey and challenges* in International Journal of Computer Networks, vol. 57, pp: 1344-1371, April 2013.

[4] X. Liang, X. S. Shen and X. Lin,, *"Grs: The green, reliability, and security of emerging machine to machine communications* in IEEE Communications Magazine, vol. 49, no. 4, pp. 28-35, 2011.

[5] Maged Hamada Ibrahim,*Maged Hamada Ibrahim, Octopus: An Edge-Fog Mutual Authentication Scheme*in International Journal of Network Security, vol.18, no.6, pp: 1089-1101, Nov. 2016.

[6] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, *Edge computing: Vision and challenges*in IEEE Internet Things Journal, vol. 3, no. 5, pp: 637-646, Oct. 2016.

[7] Atzori, L., Iera, A., Morabito, G, *The internet of things: A survey*in Journal of Computer Networks, vol. 54, no. 15, pp: 2787–2805, 2010.

[8] O. Osanaiye, S. Chen, Z. Yan, R. Lu, K. K. R. Choo, and M. Dlodlo,*From Cloud to Fog Computing: A Review and a Conceptual Live VM Migration Framework*in Special Section on Recent Advances in Cloud Radio Access Networks, vol. 5, pp: 8284–8300, 2017.

[9] Mithun Mukherjee, Rakesh Matam, Shu Leandros Maglaras, Mohamed Amine Ferrag, Nikumani Choudhury and Vikas Kumar,*Security and Privacy in Fog Computing: Challenges* in Intelligent Systems for the Internet of Things Journal, vol. 5, pp: 19293 – 19304, 2017.

[10] S. Sarkar, S. Chatterjee, and S. Misra,*Assessment of the Suitability of Fog Computing in the Context of Internet of Things*in IEEE Transactions on Cloud Computing, vol. 6, no.1, pp: 46 – 59, 2018.

[11] Saad Khan, Simon Parkinson and Yongrui Qin, *Fog computing security: a review of current applications and security solutions* in Journal of Cloud Computing: Advances, Systems, and Applications, vol. 6, no.19, 2017.

[12] Pengfei Hu, Sahraoui Dhelim, Huansheng Ning and Tie Qiu,*Survey on Fog computing: architecture, key technologies, applications, and open issues* in Journal of Network and Computer Applications, vol.98, pp: 27–42, 2017.

[13] S. Anwar, Jasni Mohamad Zain, Mohamad Fadli Zolkipli, Zakira Inayat, Suleman Khan, Bokolo Anthony and Victor Chang , *From intrusion detection to an intrusion response system: Fundamentals, requirements, and future directions* in Security and Privacy in Cloud Computing Environments, vol. 10, no. 2, pp. 1-24, Mar. 2017.

[14] I. Stojmenovic and S. Wen, *The Fog computing paradigm: Scenarios and security issues* in Proceedings of Federated Conference on Computer Science and Information Systems (FedCSIS), pp. 1-8, Sep. 2014.

[15] Arwa Alrawais, Abdulrahman Alhothaily, Chunqiang Hu and Xiuzhen Cheng, *Fog Computing for the Internet of Things: Security and Privacy Issues* in IEEE Internet Computing, vol. 21, no. 2, March 2017.

[16] Jun Zhou, Zhenfu Cao, Xiaolei Dong and Athanasios V. Vasilakos, *Security and Privacy for Cloud-Based IoT: Challenges, Countermeasures, and Future Directions* in IEEE Communications Magazine, vol. 55, no. 1, January 2017.

[17] Mohammad Alshehri and Farookh Khadeer Hussain, *A Centralized Trust Management Mechanism for the Internet of Things (CTM-IoT)* in Proceedings of the 12th International Conference on Broad-Band Wireless Computing, Communication and Applications, Barcelona, Spain, 8–10 November 2017.

[18] Mohammad Aazam, Eui-Nam Huh, *Fog Computing and Smart Gateway Based Communication for Cloud of Things* International Conference on Future Internet of Things and Cloud, 27-29 August 2014.

[19] Amandeep Singh Sohal, Rajinder Sandhu, Sandeep K. Sood, and Victor Chang, *A Cybersecurity framework to identify*

malicious edge device in Fog computing and Cloud-of-things environments in Article in Computers & Security, 2017.

[20] Arij Ben Amor, Mohamed Abid, Aref Meddeb, *A Privacy-Preserving Authentication Scheme in an Edge-Fog Environment* in IEEE/ACS 14th International Conference on Computer Systems and Applications, 2017.

[21] Eva Marín-Tordera, Xavi Masip-Bruin, Jordi García-Almiñana, Admela Jukan, Guang-Jie Ren and Jiafeng Zhu,*Do we all really know what a Fog node is? Current trends towards an open definition* in Journal of Computer Communications, vol. 109, pp: 117–130, September 2017.

[22] Shahid Raza, Tómas Helgason, Panos Papadimitratos and Thiemo Voigt,*SecureSense: End-to-End secure communication architecture for the Cloud-connected Internet of Things* in Future Generation Computer Systems, vol. 77, pp: 40–51, 2017.

[23] Antonio Escobar and Matthias Eberl,*Cloud, Fog, and Edge: Cooperation for the Future?* in IEEE Second International Conference on Fog and Mobile Edge Computing (FMEC), 2017.

[24] Bidyut Mukherjee, Roshan Lal Neupane and Prasad Calyam,*End-to-End IoT Security Middleware for Cloud-Fog Communication* in IEEE 4th International Conference on Cyber Security and Cloud Computing, 2017.

[25] Tiago Cruz, Luis Rosa, Jorge Proença, Leandros Maglaras, Matthieu Aubigny, Leonid Lev, Jianmin Jiang, and Paulo Simões,*A Cyber Security Detection Framework for Supervisory Control and Data Acquisition Systems* in IEEE Transactions on Industrial Informatics, vol. 12, no. 6, pp. 2236-2246, December 2016.

[26] Yunguo Guan, Jun Shao, Guiyi Wei, and Mande Xie,*Data Security and Privacy in Fog Computing* in IEEE Early Access Articles, vol. pp. no. 99, pp: 1-6,2018.

[27] Ali Mohammad Saghiri, Monireh Vahdati, and Kamran Gholizadeh,*A Framework for Cognitive Internet of Things based on Blockchain* in 4th International Conference on Web Research (ICWR), 2018.

[28] Y. W. Law, M. Palaniswami, G. Kounga, and A. Lo,,*WAKE: Key Management Scheme for Wide-Area Measurement Systems in Smart Grid,* in IEEE Commun. Mag., vol. 51, no. 1, pp: 34-41, Jan. 2013.

[29] Khaled Salah, Minhaj Ahmad Khan ,*IoT Security: Review, Blockchain Solutions and Open Challenges* in Future Generation Computer Systems 82, pp: 395-411, November 26, 2017.

[30] J. Granjal, E. Monteiro, J.S. Silva ,*Network-layer security for the Internet of Things using TinyOS and BLIP* in International Journal of Communication Systems, 27 (10) , pp: 1938–1963, 2014

[31] Shahid Raza, Simon Duquennoy, Tony Chung, Dogan Yazar, Thiemo Voigt, and Utz Roedig,*Securing Communication in 6LoWPAN with Compressed IPsec* in International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS), pp. 1–8, 2011.

[32] J. Granjal, E. Monteiro, J.S. Silva,*Enabling network-layer security on IPv6 wireless sensor networks* in 2010 IEEE Global Telecommunications Conference GLOBECOM 2010, pp: 1–6, 2010.

[33] P.N. Mahalle, B. Anggorojati, N.R. Prasad, R. Prasad,*Identity authentication and capability-based access control (ICAC) for the internet of things* in J. Cyber Security. Mobility 1 (4), pp: 309–348, 2013.

[34] D.U. Sinthan, M.-S. Balamurugan ,*Identity authentication and capability-based access control (IACAC) for the Internet of Things* in JCyber Secur. Mob.1 (4), pp: 309–348, 2013.

[35] M. Brachmann, O. Garcia-Morchon, M. Kirsche ,*Security for practical CoAP applications: Issues and solution approaches* in10th GI/ITG KuVS Fachgespraech Sensornetze (FGSN 2011), 2011.

[36] J. Granjal, E. Monteiro, J.S. Silva ,*End-to-end transport-layer security for internet-integrated sensing applications with mutual and delegated ecc public-key authentication* inIFIP Networking Conference, pp.1–9, 2013.

[37] G. Peretti, V. Lakkundi, M. Zorzi ,*BlinkToSCoAP: An end-to-end security framework for the Internet of Things* in 7th International Conference on Communication Systems and Networks (COMSNETS), pp. 1–6, 2015.

[38] S. Raza, T. Voigt, V. Jutvik ,*Lightweight IKEv2: a key management solution for both the compressed IPsec and the IEEE 802.15. 4 security* in Proceedings of the IETF Workshop on Smart Object Security, vol. 23, 2012.

[39] R. Riaz, K.-H. Kim, H.F. Ahmed ,*Security analysis survey and framework design for IP connected LoWPANs* in International Symposium on Autonomous Decentralized Systems, pp. 1–6, 2009.

[40] D. Conzon, T. Bolognesi, P. Brizzi, A. Lotito, R. Tomasi, M.A. Spirito ,*The VIRTUS middleware: An XMPP based architecture for secure IoT communications* in 21st International Conference on Computer Communications and Networks, ICCCN, 2012, pp. 1–6.

[41] C.H. Liu, B. Yang, T. Liu ,*Efficient naming, addressing and profile services in Internet-of-Things sensory environments* in Ad Hoc Netw. 18 (Suppl. C), pp: 85–101,2014.

[42] S. Kent ,*RFC 4302 - IP authentication header* 2005. https://tools.ietf.org/html/rfc4302.

[43] S. Kent ,*RFC 4303 - IP Encapsulating Security Payload (ESP)* 2005. https://tools.ietf.org/html/rfc4303.

[44] S. Raza, T. Chung, S. Duquennoy, D. Yazar, T. Voigt, U. Roedig ,*Securing Internet of Things with Lightweight IPsec* in SICS, Lancaster University, UK, 2011. URL http://soda.swedishict.se/4052/2/reportRevised.pdf.

[45] S. Raza, S. Duquennoy, J. Hglund, U. Roedig, T. Voigt ,*Secure Communication for the Internet of Things–a comparison of link-layer security and IPsec for 6LoWPAN* in Secur. Commun. Netw. 7 (12), pp: 2654–2668, 2014.

[46] J.W. Hui, P. Thubert ,*Compression Format for IPv6 Datagrams in 6LoWPAN Networks draft-IETF-6lowpan-hc-13* 2010. https://tools.ietf.org/html/draft-ietf-6lowpan hc-13.

[47] T. Kothmayr, C. Schmitt, W. Hu, M. Brnig, G. Carle ,*A DTLS based end-to-end security architecture for the Internet of Things with two-way authentication* in 37th Annual IEEE Conference on Local Computer Networks - Workshops, pp. 956–963, 2012.

[48] T. Kothmayr, C. Schmitt, W. Hu, M. Brnig, G. Carle ,*DTLS based security and two-way authentication for the Internet of Things* in Ad Hoc Netw. 11 (8) (2013) 2710–2723.

[49] S.L. Kinney ,*Trusted Platform Module Basics: Using TPM in Embedded Systems* in Newnes, Newton, MA, USA, 2006.

[50] X. Huang, Y. Xiang, E. Bertino, J. Zhou, L. Xu ,*Robust multi-factor authentication for fragile communications* in IEEE

Trans. Dependable Secure Comput. 11 (6), pp: 568–581, 2014.

[51] S. Raza, S. Duquennoy, T. Chung, D. Yazar, T. Voigt, U. Roedig,*Securing Communication in 6LoWPAN with Compressed IPsec* in International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS), 2011, pp. 1–8.

[52] M. Henze, B. Wolters, R. Matzutt, T. Zimmermann, K. Wehrle ,*Distributed configuration, authorization and management in the cloud-based internet of things* in IEEE Trustcom/BigDataSE/ICESS, pp: 185–192, 2017.

[53] J. Zhou, Z. Cao, X. Dong, A.V. Vasilakos ,*Security and privacy for cloud-based IoT: Challenges* in IEEE Commun. Mag. 55 (1), pp: 26–33, 2017.

[54] J.M. Bohli, A. Skarmeta, M.V. Moreno, D. Garca, P. Langendörfer,*SMARTIE project: Secure IoT data management for smart cities* in International Conference on Recent Advances in Internet of Things (RIoT), pp: 1–6, 2015.

[55] A.A. Chavan, M.K. Nighot ,*Secure CoAP using enhanced DTLS for the Internet of Things* in Internat. J. Innovative Res. Comput. Commun. Eng. 2 (12), 7601–7608, 2014.

[56] S. Raza, D. Trabalza, T. Voigt, "6LoWPAN compressed DTLS for CoAP in IEEE 8th International Conference on Distributed Computing in Sensor Systems, pp: 287–289, 2012.

[57] R. Harkanson, Y. Kim ,*Applications of elliptic curve cryptography: A light introduction to elliptic curves and a survey of their applications* in Proceedings of the 12th Annual Conference on Cyber and Information Security Research, CISRC '17, ACM, New York, NY, USA, pp: 6:1–6:7, 2017.

[58] A. Gmez-Goiri, P. Ordua, J. Diego, D.L. de Ipiña ,*Otsopack: Lightweight semantic framework for interoperable ambient intelligence applications* in Comput. Hum. Behav. 30 (Suppl. C), pp: 460–467, 2014.

[59] H.G.C. Ferreira, R.T. de Sousa, F.E.G. de Deus, E.D. Canedo ,*Proposal of a secure, deployable and transparent middleware for the Internet of Things* in 9th Iberian Conference on Information Systems and Technologies, CISTI, pp: 1–4, 2014.

[60] J. Granjal, R. Silva, E. Monteiro, J.S. Silva, F. Boavida ,*Why is IPSec a viable option for wireless sensor networks* in 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, pp: 802–807, 2008.

[61] A.Bahga, V.K.Madisetti ,*Blockchain Platform for Industrial Internet of Things* in Tech.Rep.2016. URL http://file.scirp.org/pdf/JSEA_2016102814012798.pdf.

[62] K. Christidis, M. Devetsikiotis ,*Blockchains and smart contracts for the InternetofThings* in IEEEAccess4, pp: 2292–2303, 2016.

[63] V. Pureswaran, P. Brody ,*Device Democracy - Saving the future of the Internet of Things* i IBM, 2014. http://www 01.ibm.com/common/ssi/cgibin/ssialias?htmlfid=GBE03620USEN.

[64] P. Kamalinejad, C. Mahapatra, Z. Sheng, S. Mirabbasi, V.C.M. Leung, Y.L. Guan ,*Wireless energy harvesting for the Internet of Things* in IEEE Commun. Mag. 53 (6), 2015, pp: 102–108.

[65] X.Li, P.Jiang, T.Chen, X.Luo, Q.Wen,*A Survey on the Security of Blockchain Systems* in Future Gener. Comput. Syst. ,2017.

[66] I. Friese, J. Heuer, N. Kong ,*Challenges from the Identities of Things: Introduction of the Identities of Things discussion group within Kantara initiative* in IEEE World Forum on Internet of Things (WF-IoT), pp: 1–4, 2014.

[67] P. Otte, M. de Vos, J. Pouwelse ,*TrustChain: A Sybil-resistant scalable Blockchain* in Future Gener. Comput. Syst., 2017.

[68] Mayra Samaniego, Uurtsaikh Jamsrandorj and Ralph Deters ,*Blockchain As a Service for IoT* in IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp: 433-436, 2016.

[69] Nakamoto, Satoshi ,*Bitcoin: A peer-to-peer electronic cash system*, 2008.

[70] Oscar Novo ,*Blockchain meets IoT: An Architecture for scalable Access Management in IoT* in Journal of Internet of Things Class Files, vol. 14, no. 8, March 2018.

[71] Nallapaneni Manoj Kumar, Archana Dash, Neeraj Kumar Singh ,*Internet of Things (IoT): An Opportunity for Energy-Food-Water Nexus* in 1st IEEE International Conference on Power Energy, Environment & Intelligent Control (PEEIC2018), GL Bajaj, Greater Noida, India, 13th and 14th April 2018.

[72] S. Hernan, S. Lambert, T. Ostwald, and A. Shostack,*Uncover security design flaws using the STRIDE approach* in MSDN Magazine, Nov. 2006.

[73] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman ,*Towards a Novel Privacy-Preserving Access Control Model Based on Blockchain Technology in IoT* in Cham: Springer International Publishing, pp: 523–533, 2017.

[74] Nallapaneni Manoj Kumara and Pradeep Kumar Mallick ,*Blockchain technology for security issues and challenges in IoT* in International Conference on Computational Intelligence and Data Science (ICCIDS 2018), 132, pp: 1815–1823, 2018.

[75] Seyoung Huh, Sangrae Cho and Soohyung Kim ,*Managing IoT devices using Blockchain platform* in ICACT2017 February 19 -22, 2017.

[76] Nabil Rifi, Elie Rachkidi, Nazim Agoulmine and Nada Chendeb Taher ,*Towards using Blockchain Technology for IoT data access protection* in IEEE 17th International Conference on Ubiquitous Wireless Broadband (ICUWB), 12-15 Sept. 2017.

[77] Sayed Hadi Hashemi, Faraz Faghri, Paul Rauschy and Roy H Campbell ,*World of Empowered IoT Users* in IEEE First International Conference on Internet-of Things Design and Implementation (IoTDI), 2016.

[78] Matthias Mettler, M.A. HSG Boydak ,*Blockchain Technology in Healthcare The Revolution Starts Here* in IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), 2016.

[79] Asaph Azaria, Ariel Ekblaw, Thiago Vieira and Andrew Lippman ,*MedRec: Using Blockchain for Medical Data Access and Permission Management* in International Conference on Open and Big Data (OBD), 2016.

[80] Jie Zhang, Nian Xue, and Xin Huang ,*A Secure System For Pervasive Social Network-Based Healthcare* in IEEE Access Volume: 4, pp: 9239 – 9250, 2016.
[81] Zyskind, Guy, and Oz Nathan,*Decentralizing privacy: Using Blockchain to protect personal data* in In Security and Privacy Workshops (SPW), IEEE, pp: 180-184, 2015.
[82] *IPFS - Content Addressed, Versioned, P2P File System*, https://ipfs.io/docs/ (Last accessed on 15 may 2020)
[83] Anasuya Acharya, Manoj Prabhakaran and Akash Trehan,*Cell Tree: A New Paradigm for Distributed Data Repositories* May 17,2019.
[84] Adam Back, Matt Corallo, Luke Dashjr, Mark Friedenbach, Gregory Maxwell, Andrew Miller, Andrew Poelstra, Jorge Timón, and Pieter Wuille ,*Enabling Blockchain innovations with pegged sidechains* https://blockstream.com/sidechains. pdf, 2014.
[85] Joseph Poon and Thaddeus Dryja ,*The bitcoin lightning network: Scalable off-chain instant payments* 14, 01, 2016. https://lightning.network/ lightning-network-paper.pdf
[86] *Cardano* 2015. https://www.cardano.org
[87] Yossi Gilad, Rotem Hemo, Silvio Micali, Georgios Vlachos, and Nickolai Zeldovich ,*Algorand: Scaling byzantine agreements for cryptocurrencies* In Proceedings of the 26th Symposium on Operating Systems Principles, pp: 51–68. ACM, 2017.
[88] Aggelos Kiayias, Alexander Russell, Bernardo David, and Roman Oliynykov ,*Ouroboros: A provably secure proof-of-stake Blockchain protocol*. In CRYPTO, Springer International Publishing, pp: 357 388, 2017.
[89] Leemon Baird, Mance Harmon, and Paul Madsen ,*Hedera: A governing council and public hashgraph network* 2017. https://www.hederahashgraph.com/whitepaper
[90] Serguei Popov ,*The tangle* 2017 http://iotatoken.com/ IOTA_Whitepaper.pdf
[91] RomanMatzutt, JensHiller, MartinHenze, JanHenrik Ziegeldorf, Dirk Müllmann, Oliver Hohlfeld, and Klaus Wehrle,*A quantitative analysis of the impact of arbitrary Blockchain content on bitcoin*in 2018.
[92] D.Eastlake, P.E.Jones,*RFC3174-US Secure Hash Algorithm1 (SHA1)* 2001. URLhttps://tools.ietf.org/html/rfc3174
[93] Dr. B. V. Ramana Reddy,*Blockchain: A Game changer for securing IoT Data* in Volume 8, Issue 5, pp: 580-588, MAY 2019.
[94] Siegel, D.,*Understanding the DAO Hack for Journalists* https://medium.com/@pullnews/understanding-the-dao-hack-for-journalists-2312dd43e99(Last accessed on 15 may 2020)
[95] Xiaoqi Lia, Peng Jianga, Ting Chenb, Xiapu Luoa, and Qiaoyan Wenc,*A Survey on the Security of Blockchain Systems* 6 Mar 2018. https://arxiv.org/pdf/1802.06993.pdf
[96] *Block chain developer course* https://vomtom.at (Last accessed on 15 may 2020)
[97] *WWW.Ethereum.org*(Last accessed on 15 may 2020)
[98] *Understanding How Blockchain Works*
https://blog.ndcconferences.com/understanding-Blockchain/ (Last accessed on 15 may 2020)
[99] *Slock.it* https://slock.it (Last accessed on 15 may 2020)
[100] *TransactiveGrid* http://transactivegrid.net (Last accessed on 15 may 2020)
[101] *Filament (2016) Foundations for the Next Economic Revolution Distributed Exchange and the Internet of Things* https://filament.com/assets/downloads/Filament
[102] *Blockchain adoption could help in COVID-19 fight* https://www.bioworld.com/articles/435042-blockchain-adoption-could-help-in-covid-19-fight (Last accessed on 15 may 2020)
[103] *Blockchain and Corona virus: could it prevent future pandemics* https://www.finextra.com/blogposting/18570/blockchain-and-corona-virus-could-it-prevent-future-pandemics (Last accessed on 15 may 2020)
[104] Andrea, I., Chrysostomou, C., Hadjichristofi, G.,*Internet of things: security vulnerabilities and challenges*in 2015 IEEE Symposium on Computers and Communication (ISCC), pp. 180–187, 2015.
[105] Ahemd, M.M., Shah, M.A., Wahid, A,*Iot security: a layered approach for attacks and defenses* in 2017 International Conference on Communication Technologies (ComTech), pp. 104–110, 2017.
[106] Aman, M.N., Chua, K.C., Sikdar, B.,*A light-weight mutual authentication protocol for iot systems* in GLOBECOM 2017 - 2017 IEEE Global Communications Conference, pp. 1–6, 2017.
[107] Porambage, P., Schmitt, C., Kumar, P., Gurtov, A., Ylianttila, M.,*Pauthkey: a pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed iot applications* in Int. J. Distributed Sens. Netw. 10 (7), 357430, 2014. https://doi.org/10.1155/2014/357430
[108] Aman, M.N., Chua, K.C., Sikdar, B.,*A light-weight mutual authentication protocol for iot systems* in GLOBECOM 2017 - 2017 IEEE Global Communications Conference, pp: 1–6, 2017.
[109] Choi, J., Kim, Y.,*An improved lea block encryption algorithm to prevent side-channel attack in the iot system* in 2016 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA), pp. 1–4, 2016.
[110] Liu, J., Zhang, C., Fang, Y.,*Epic: a differential privacy framework to defend smart homes against internet traffic analysis*in IEEE Internet Things J. 5 (2), pp: 1206–1217, 2018.
[111] Guin, U., Singh, A., Alam, M., Caedo, J., Skjellum, A.,*A secure low-cost edge device authentication scheme for the internet of things* in 31st International Conference on VLSI Design and 17th International Conference on Embedded Systems (VLSID), pp: 85–90, 2018.
[112] Varga, P., Plosz, S., Soos, G., Hegedus, C.,*Security threats and issues in automation iot* in 2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS), pp:. 1–6, 2017.
[113] Glissa, G., Rachedi, A., Meddeb, A.,*A secure routing protocol based on rpl for internet of things* in IEEE Global Communications Conference (GLOBECOM), pp. 1–7, 2016.
[114] Pu, C., Hajjar, S.,*Mitigating forwarding misbehaviors in rpl-based low power and lossy networks* in 2018 15th IEEE Annual

Consumer Communications Networking Conference (CCNC), pp: 1–6, 2018.
[115] Cervantes, C., Poplade, D., Nogueira, M., Santos, A.,*Detection of sinkhole attacks for supporting secure routing on 6lowpan for internet of things* in 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), pp: 606–611, 2015.
[116] Singh, M., Rajan, M.A., Shivraj, V.L., Balamuralidhar, P.,*Secure mqtt for internet of things (iot)*in: 5th International Conference on Communication Systems and Network Technologies, pp. 746–751, 2015.
[117] Park, N., Kang, N.,*Mutual authentication scheme in secure internet of things technology for comfortable lifestyle*in Sensors 16 (1), 2015.
[118] Ashibani, Y., Mahmoud, Q.H.,*An efficient and secure scheme for smart home communication using identity-based signcryption.*in 2017 IEEE 36th International Performance Computing and Communications Conference (IPCCC), pp: 1–7, 2017.
[119] Chan, M.,*Why Cloud Computing Is the Foundation of the Internet of Things* 2017. https://www.thorntech.com/2017/02/cloud-computing-foundation-internetthings/.
[120] Song, T., Li, R., Mei, B., Yu, J., Xing, X., Cheng, X.,*A privacy preserving communication protocol for IoT applications in smart homes* in IEEE Internet Things J. 4 (6), 1844–1852, 2017.
[121] Machado, C., Frhlich, A.A.M.,*Iot data integrity verification for cyber-physical systems using blockchain* in 2018 IEEE 21st International Symposium on Real-Time Distributed Computing (ISORC), pp. 83–90, 2018.
[122] Rahulamathavan, Y., Phan, R.C., Rajarajan, M., Misra, S., Kondoz, A.,*Privacy-preserving blockchain based iot ecosystem using attribute-based encryption*in IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), pp. 1–6, 2017.
[123] Zheng, D., Wu, A., Zhang, Y., Zhao, Q., *Efficient and privacy-preserving medical data sharing in internet of things with limited computing power* in IEEE Access 6, 28019–28027, 2018.
[124] Gope, P., Sikdar, B.,*Lightweight and privacy-preserving two-factor authentication scheme for iot devices.* in IEEE Internet Things J.. 2018.
[125] Gai, K., Choo, K.R., Qiu, M., Zhu, L.,*Privacy-preserving content-oriented wireless communication in internet-of-things.*in IEEE Internet Things J. 5 (4), 3059–3067, 2018. [126]
[126] Sengupta, J., Ruj, S., Bit, S.D.,*End to end secure anonymous communication for secure directed diffusion in iot.* in Proceedings of the 20th International Conference on Distributed Computing and Networking, ICDCN '19, pp. 445–450, 2019. https://doi. org/10.1145/3288599.3295577.
[127] Jayasree Sengupta, Sushmita Ruj and Sipra Das Bit,*A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT.*in Journal of Network and Computer Applications, 30 oct 2019.
[128] Syed Rameem Zahra and Mohammad Ahsan Chisht,*Assessing the Services, Security Threats, Challenges and Solutions in the Internet of Things.*in Scalable Computing: Practice and Experience, Vol 20, Number 3, pp 457-484, 30 Aug 2019.
[129] *Five ways in which Blockchain technology can aid a recover* https://www.livemint.com/opinion/columns/five-ways-in-which-blockchain-technology-can-aid-a-recovery-11589479234967.html (Last accessed on 15 may 2020)
[130] Rahul K. Garg, *Is Blockchain in Indian healthcare worth the challenges* https://health.economictimes.indiatimes.com/news/health-it/is-blockchain-in-indian-healthcare-worth-the-challenges/64095898 (Last accessed on 15 may 2020).

Edited by: Anand Nayyar
Received: Jun 12, 2020
Accepted: Jul 17, 2020