1. LITERATURE REVIEW

2.1 Adrian Perrig et. al., (2002), proposed a security protocol for sensor network optimization using SPINS. The paper explores the challenges for security in sensor network by building a small prototype network called SmartDust program. The main challenge was to broadcast authenticated data to the entire network. Spins had two blocks SNEP that provided data confidentiality between 2 parties authentication, integrity and freshness, while µ TESLA (micro Tesla) provide authentication broadcasting using asymmetric mechanism. All message cryptographic algorithms provides necessary information. Freshness in an algorithm is provided by a random number generator that is used in it. An evaluation of its implementation was done on code size, RAM size, processor and communication overheads. The author demonstrated to build secure protocol on a authentication routing application and 2 Key agreement protocol.

2.2 IF Akyildin et al.,(2002), in their paper describes the concept of sensors networks as the convergence of micro-electrical mechanism system technology, wireless communication and digital electronics. From what is a sensing task to application in sensor network like military, environment, health, home and commercial area are explores by the authors. Their study included the factor influencing the design of the sensor network that includes fault tolerance, scalability, production cost, operating environment, sensor network topology, hardware, transmission media and power consumption. On detail investigation of the current proposals the sensor network protocol stack was developed with all the algorithms and protocol needed. The author discusses the MAC protocol with the WINS network along with the other protocols based in the different layers. They conclude with open research issues like power efficiency, transceiver design to modulation schemes.

2.3 Chee -Yee Chong and Srikanta P. Kumar , (2003), traces the history of sensor networks from the development point of view of sensing, communication and computing. In 21th century a network of SensIT nodes and TASS (tactical automated security system) was used, they detected, identified the target and dynamically give tasks, query and tackle threats. With the emergence of new technologies, the authors noticed that new technical problems of infrastructural security, habitat and environment monitoring, industrial sensing and traffic control. The challenges at the network level were Adhoc network discovery,
Control routing packets, Collaborative signal and Information processing, Tasking, Queueing and Security. The DARPA SecIT provides solution and areas of new research like Localization, Direct diffusion and distributed tacking in Wireless Adhoc Network using Mobile agents for distributed classification the performance and the efficiency would improve in wireless sensor networks.

2.4 Xiaojiang Du et. al., (2008), summarizes a list of 12 attacks on WSN and set out two assumptions that the base station is always protected and trusted, and if attacked the entire sensor network will fail, therefore keeping its secure is a necessity. The author suggests that the entire network could provide basic functionalities with minimal degradation, the paper describes the security issues of key management, secure time synchronization deals with sensing, tracking, scheduling sensor, mobile object tracking and TDMA. The NTP, the Reference broadcast synchronization, time synchronization protocol is used for sensor network. The authors identify four possible attacks on sensor time synchronization Masquerade attack., Relay attack., message manipulation attack, delay attack. The location discovery protocol plays an important role in environment monitoring and target tracking with beacon nodes and GPS receivers for with secure routing use essential for a heterogenous sensor network.

2.5 Rolf H. Weber , (2010) in his paper considered the measure ensuring the architecture resilience at attacks, data authentication, access control and client privacy. Considering the IoT notation, the technical background and listing of the privacy enhancing technologies like VPN, TLS, DNSSec the author establishes and implements an appropriate legal framework called a systematic approach in relation with the legislative process which considered the facts of using an RFID scenario provided by guidance on the design and operation bringing out a PIA report in 2009. It has systemization of legal probe under four technical areas globality, verticality, ubiquity and technicity. The author systemized the challenges of security related to RFID and IoT for qualitatively classified based on the EU directives, it encompasses privacy and data protection of personal data created from IoT devices, which soon became applicable to all member states.

2.6 Debasis Bandyopadhyya and Jaydip Sen , (2011), in their paper the author introduces a Internet layer in between the upper half that has application and middleware layers that
handled network services while the lower layers were Edge, Access gateway and the Network Layer. The authors list out 12 technologies which enables IoT for identification technology to security and privacy technology, including standardization which has International Standard for Metadata Registries and its implementation. The Universal Data Element Framework supports interoperability between the structure data of different schema by providing a global unique cross reference identifier for data elements that are schematically equivalent. The IETF related all IoT IPv6 over 6LoWPAN which define a set of protocol in IPv6. The middleware technology and the Relationship Network management manages the distributed database and auto pooling of network devices and real time graphical view. The author sites potential growth in the intelligent application from smart homes to smart enterprise and factories.

2.7 HuiSuo, JiaFoWan et. al.,(2012), in their presentation talks on IoT as cyber transportation system cyber physical system and machine to machine communication system which need new technologies and methodologies to meet the higher need of security and privacy. They describe the four key layers of the IoT in terms of security architecture and the requirements tools used to secure them with necessary mechanism like encryption and recovery. The paper recommends encryption mechanism at each hop, TLS/SSL agents to evade DDOS attacks, a recovery mechanism if attacked, protecting private sensitive data of individual sensors and implementation cryptographic algorithm in a small space of memory in the devise with low processing speed are the areas for critical research. The paper summarizes security structure, implementation of defense in depth of the, key management and algorithms of cryptography in low memory, processors in sensors and policy improvements are the new challenges faced by the security of IoT with the development of new technologies.

2.8 Rodrigo Roman et. al.,(2013), describes the IoT service as services proposed by centralised architecture, but exchange of information and collaboration of entities is done keeping distributed architecture. On focus based on the principle of Edge intelligence and Collaboration there are four approaches Centralized IoT , Collaborative IoT , Connected Intranet of Things , and Distributed IoT. The analysis of the properties and the requirements of the centralized IoT . In the next section the author provides overview generic problem in
security of Distributed IoT Principles and analysis the attacker models and threats. The Access control mechanism and a distributed IDS are recommended for detecting outliers in a clustered based approach derived from a centralised IoT. At the end the author specifies a table with all the challenges like Identification and Authentication, Access Control protocols and Network Security, Privacy. Trust, Governance and fault tolerance for Centralised IoT and Distributed IoT.

2.9 Xu Xiaodui, (2013), in this paper studies the security problems of the rapidly developing IoT network. It gives an overview of the composition of the IoT layers and its developments for information perception, intelligence material and intelligence interaction and describing the various type of attacks classifying security as terminal security in future for authentication, sensor network security , information transmission security, processing safety and business security as the problem for security , to which the author makes recommendation for certification of identity (PKI), Data encryption, a good middleware could handle operation in different technologies hiding details of underlying different technologies but managing trust, privacy and security of all exchange of data while cloud computing could be used for intelligence processing.

2.10 S.Sicari et. al., (2015), outlines six survey contribution of research papers that are factors that affect IoT security. The first is the requirement of IoT as authentication, confidentiality and control, where authentication and confidentiality The Second is privacy IoT. The third is Trust in IoT that adopt a dynamic trust management policy capable of best trust factor in a dynamic environment with maximum performance. The fourth is Enforcement of policy on IoT that force applications on IoT with a set of defined action in a system or operation rules to maintain order . The fifth is securing a Middleware in IoT to enforce integration and security of the device and data between platforms. (XMPP, Ami framework called Otsopack, OneM2M as a global service platform). Finally, the ongoing projects Hydra Project, EU FP7 Project, iCore project, uTrustit are some of them.

2.11 Tuhin Borgohain et. al., (2015), analysis the privacy issues of the end-users encountered as and spread of IoT. The automatic exchange of information between two IoT devices are possible due to connectivity technologies like WSN and RFID which posed a risk to several security issues of CIA. The author studies the effect of a DOS attack on all layers of TCP/IP
stack, thus specifying the attack on the availability of the network as the security and privacy concerns to IoT. The author describes fourteen types of DOS attack in WSN. They also list out the attack on CIA of IoT with the RFID technology some of which were unautistic tag tracking, tag cloning, disabling and replay attack showing how they are vulnerable to attacks. The author describes a short case study on security of Health-related technology built on the concept of IoT.

2.12 Authur Gervais et. al., (2016), describe how Proof of Work (PoW) as a consensus mechanism is related to block interval, smaller the block interval faster the inter action and greater the probability of stale block. Lowering the difficulty layer of the number of blocks in the chain, greater are the chances of being attacked. The Self Mining attack is described as a security problem at block security. The author use Markov Distribution process for describing security model for an elliptical attack using a single player decision model which is transposed to all user that participate in the same standard protocol $S$ : $(I_a, I_b, b_c, fork)$. The author mathematically proves the optimal strategy for self-mining and policy iteration algorithms for double spending. The author observes to enable the security implication and observes that the Ethereum is weaker to Bitcoin as Bitcoin has a stronger uniform tie tracking and uncle rewards. Using a Blockchain simulator that has regular modes and miners the author evaluates and validates the impact of block interval, block size and properties in form of tables and graph.

2.13 Beck et al., (2016), in their suggest the Ethereum blockchain communicates with Smart objects devices through smart contracts, serves as the back-end of decentralized applications, where everyone to write smart contracts to build your own rules. the blockchain is a “trust-free”, distributed solution that can be understood as techno-social system, where the technical part assures the transactions of the social part, which cannot be altered as long as the transaction takes place under the conditions of the agreed upon smart contract. The author creates demonstrator of a coffee self-service case which was based on proof of concept which is the solution of trust-base self-service system at the shop. This is like the concept of Smart contract that operates on the network, the application could be decentralized. The analysis is done through unit testing, functional testing, apply boundary condition. The author notices few difficulties that there is no uniform transaction language inn different systems, the block
time factor as it is decentralized an soon users will have to pay for the servers and services there it has hidden cost.

2.14 Deepak P Uthal et al., (2016), the authors notices that in Big Data Analytics there is an exchange of data from the edge data centers (EDC) to the cloud data centers (CDC) through all the architecture layers. With unsupervised activity there is a chance of being attacked or even threat of attacks at each layer. The paper provide solution to ensure end to end security and privacy of data between the EDC and CDC. The attack could take place at the perception devices ie. sensors or at the actuators level. The authors notice there were attacks at the integration of sensor and network on the software frameworks and hardware resources, hence the network layer security problem and solution are considered at the EDC and the application layer security problem and solution are considered at the CDC. The authors recommend the industries 3 approaches Zero trust ie, never trust, always verify with the EDC and CDC, “deperimeterization” ie. hardened perimeter security for multi-layered EDC and CDC and perimeter software encryption for authentication and authorization. There is an urgent need to secure the data at the EDC as the software solutions handle threats at the CDC.

2.15 Jatinder Singh et. al., (2016), noticed that data security in cloud computing was an inhabited on to the cloud service for different sectors and organizations. The cloud had services to hold and process the data of, manage components and combine data stream of “things”. The authors provide twenty considerations with a broad consensus of issues of accessing the cloud, data management in the cloud through services and management of the cloud, issues associated with identity management, scalability issues in IoT cloud, security issues form malicious things, compliance among the provider transparency and decentralization. They provide a taxonomy that considers the above the CIA security principles, the current status of technologies used, the working need of the problem understood and extension of the research need to understand and solve the problems.

2.16 Jesse Yil Hummo et. al., (2016), conducting a systematic mapping study with the goal of collecting all relevant research papers in Block technology. The authors primary observed the from 41 types primary papers were of scientific data uses, 80% of the papers were on Bitcon and 20% on Bitcon Application like smart contract licensing. The relevant papers were
classified as blockchain reports, improvements and applications. 43% of the papers were related to security and impact of security incidence, 51% on attack on data malleability problems authentication and cryptography issues. The authors also identified papers that the study related to solution on wasted resource problem in blockchain and bitcoin for example running of mining hardware with high returns and power efficiency. They recognized that there were support tool to help the user to analyze the whole blockchain network to improve usability. Experimentally there was a lack of anonymity in the Bitcoin network. The traffic pattern was analyzed and a subset of Bitcoin address can be mapped to IP addresses transaction mixing techniques was used to increase privacy. The author discusses the result as answers to research question and validity to the studies carried out.

2.17 Minela Grabovica et. al., (2016), explores the RFID, optical tags, quick response codes Bluetooth, wireless networking, Zigbee, Z-wave, LTE advances and Wifi Direct as the enabling key technologies in IoT who setup communication between the devices and Internet. Each technology is explained with its layer of services and modes of security implementation on them thus proving that the security requirement is met. They also mention the constrains each technology may encounter like Zigbee will only run on devices that trust each other or Bluetooth network may be Bluejacked, Carwispered or Bluesnarfed.. The RFID and Wi-Fi are compared with the advantage and disadvantage of these Technologies.

2.18 Alexander Kuzmin (2017), in this paper the author describes OSI 7-layer model and IoT Reference Model: Security to describe the anatomy of IoT and compare Internet Protocols and IoT Protocols. The property for being public, decentralized and secure is the advantages of Blockchain Technology. The distributed infrastructure of the Blockchain and an integrated protocol of the IoT are used together on heterogeneous system in the next section of the paper the author uses standard notation and terminology of graph theory, the model too uses Ford–Fulkerson algorithm (FFA) that computes the maximum data flow in network, it reduces the amount of calculation, finding approximately minimum connected dominating set, namely, the monitoring and calculation centers of IoT. To limit block size Channel capacity was applied to DOB (Device-Of-Blockchain), which allows to geometrically increasing the integrity of configurations and exchanged IoT data. For 5G-compatible
devices Blockchain-base Structures where users on the blockchain created block by smart contracts.

2.19 Ali Doori et. al.,(2017), in this paper the authors approach was improving a smart home setting and consists of three main tiers namely: cloud storage, overlay, and smart home. The communication transactions, Basic Private Blockchain, home miner and a local store are the various core components. Each smart home has an high resource device, known as ”miner” that is always online and is responsible for handling all communication within and external to the home. The miner also preserves a private and secure Blockchain, used for controlling and auditing communications. The proposed block-based smart home framework is secure by thoroughly analysing its security through the DDOS attack and linking attack with respect to the fundamental security goals of confidentiality, integrity, and availability. They evaluated the performance bases on the transaction stored as periodic or query based and highlighting that the overheads (in terms of traffic, processing time and energy consumption) introduced by the approach are insignificant relative to its security and privacy gain.

2.20 Ali Dorri et. al., 2017 in their paper optimized Blockchain (BC) for IOT for security and privacy. Blockchain has its drawbacks as high resource consumption, scalability and processing time. In the first section BC security mainly comes from a cryptographic puzzle known as Proof of Work (POW) used for appending (mining) new blocks into the BC. BC also offers a high level of privacy by using a changeable Public Key (PK) as the users’ identity. In the second section the smart home as the use case the author adopt a hierarchical structure to optimize resource consumption and increase network scalability It uses private Immutable Ledger (IL), that acts similar to BC but is managed centrally, and symmetric encryption to reduce the processing. There is a verified signed transaction for the entire network This reduce the delay in the transactions. Distributed Trust method use the overlay to decrease processing for a new block.

2.21 Ali Kaan Koc et. al., (2017), introduces of smart contracts, as in the Ethereum platform to the new digitization of online services. Smart contracts are meaningful pieces of codes, to be integrated in the blockchain and executed as scheduled in every step of blockchain updates. E-voting is critical as its online services. The blockchain with the smart contracts, emerges as a good candidate to use in developments of safer, cheaper, more secure, more
transparent, and easier-to-use e-voting systems. The authors implemented and tested a sample e-voting application as a smart contract for the Ethereum network using the Ethereum wallets or an Android platform and the Solidity language for allowing people to vote and Ethereum blockchain will hold the records of ballots and votes. The e-voting transaction requests are handled with the consensus (creates a transparent environment) of every single Ethereum node. The author implements it on a small-scale poll with the blockchain-based e-voting systems, its test results confirms reliability and efficiency of Blockchain used for E-voting.

2.22 Fari Assaderaghi et. al., (2017), begins the paper information about the four pillars of IoT. The first are the transducers which have been developed low power sensors which are smaller size and lower in cost. The second is the edge making computing a challenge due to the latency, bandwidth and real time analytics. Therefore, there is a need to improve various type of embedded processor to handle computational capabilities and power efficiency. The third pillar being the communication infrastructure for ultra-short range, short range and low power wide area (LPWA) needed to be accelerate wireless communication based on the distance and challenges of interoperability. For the study of the forth pillar of Privacy and Security the extends the challenges of data integration, confidentiality, certification, interoperability, trust, authentication and privacy from secure system to the IoT environment. The author suggests effective counter measures to sustain security like security at end to end level considering that the system will fail at some point in time for a mobile payment system.

2.23 JeiLin Ch et. al., (2017), in the paper introduce Fog computations bases IoT for future Infrastructural development of IoT with distributed architecture. In the second section of the paper CPS (cyber physical system is system) and IoT (is internet) are integrated with smart transportation, smart grid to identify IoT device at communication layer. Describing the three layer of the IoT Architecture and a Service of Applications (SOA) Architecture model the authors describes the various enabling technologies at the perception layer and the network layer. The jobs of each are explained with the description of the key feature of security of IoT with relationship with the layers and type of attack at each in detail Privacy of the data is categorized as data collection, aggregation, analytics and mining. The integration of Fog computing and IoT is described with two equation, one to maximize the overall satisfaction
of end users and minimum delay of the cost of computation. Smart Grid, Smart Transportation, Smart Cities are some of the application of CSP/IoT.

2.24 Kishore Angrishi, (2017) in his paper the author says that the IoT will be worth $11 trillion annually but would have like poor and complex security with 9+ billion issues by 2025. This would change IoT to IoV (Internet of vulnerabilities). The author takes special interest in describing the DDoS, the protocols at DSL and BRAS traffic routing and aggregating user session from the access network, counter delivery network and DNS service provide AntiDDOS or DDoS mitigation service. The author discuss that the IoT Malware orchestrate various types DDoS attacks causing extended damage and chaos globally. Since 2016 state that here has been an increase of 138% of DDoS from 100 Gbps IoT devices. The involvement of Open Internet, ClearNet, Darknet have over 435 booster and stresser website that offer their services like DDoSaaS via IoT Botnets. The author explains the anatomy and the working of the IoT botnet and relationship between different actors involved in DDoS using IoT devices to provide hardware, legal implication on IoT device certification and insurance as solution to avoiding IoT to become IoV.

2.25 Mid Hasanmaddi and Mohammed Quyyun, (2017), in their paper describe the IoT world to be under the influence of new emerging technologies, where smart device are exposed to cyber-attacks and threats. The authors describe WSN and RFID with the list of major attack on them. As conclusion the author recommends encryption in an end to end environment, access control measure for real time and critical infrastructure. In the future there would be smart devices which would meet the security and privacy criteria to automate tasks connectivity using new technologies.

2.26 Pradip Kumar Sharma et. al. (2017), this paper proposes a novel blockchain-based distributed cloud architecture with a software defined networking (SDN) enable controller fog nodes at the edge of the network to meet the required design principles. The author attempts to bring computing resources to the edge of the IoT network through deployment of fog nodes allow quicker access to large amounts of data in a secure manner. They provide a secure distributed fog node architecture that uses SDN and blockchain technique where security must automatically adapt to the threat landscape, thus dispensing with the need for administrators to manually review and apply thousands of recommendations and opinions at
the edge of the network. On evaluation of the new model with the previous existing models it shows that performance is improved by reducing the induced delay, reducing the response time, increasing throughput, and the ability to detect real-time attacks in the IoT network with low performance overheads.

2.27 Pratesksha Varshney and Yogesh Simmha, (2017), the authors to monitor and identify the gaps posed by cloud only or edge cloud model. The author manipulates the Fog and application. This was possible through runtime and middleware capabilities. Lastly the author recognizes the task of platform interoperability as a gap and resolved it by IaaS as fog data flow inhibited loosely coupled system, the state and its location element plated an important role. The author describes a model based on distributed hash table to maintains an overlay of the network and suggested a hybrid model adapted the change in platform and handle interconnection of resources as the lower resource and the higher resource were not accessible. The author suggests future related to foglets as software agents to manage local operation and it is used as a second level to data centers, Fog and cloud are used as PaaS and helps in the coordination of distributed Edge devices.

2.28 Rajat Chaudhary et. al., (2017), in their paper describes the changes in the IoT in introducing the NSC (Network service chaining) in between the Cloud computing and Fog Computing in 5G wireless Architecture. The NSC is built of service classified controller to a SDN and network function virtualized platform for service chaining like firewall, TCP connection, NAT, Traffic signaling. The author compares XenSensor, VWare, ESG, KVM and HyperV as virtualization tool to represent physical resource by creating specimen and representation logical resources. The author describes the concept of fog abstraction node and foglet in 5G wireless network and comparts it with Cloud computing. The author purposed a security model for CloudLet Mesh and Kerberos as security authentication mechanism for it. The future work recommended by the author in the 5G Security in SDN base Cloud Infrastructure.

2.29 Sophia Moganedi and Jabu Mtsweni, (2017), give a details of the current security and privacy challenges presented by increasing use of the IoT domain based on the systematic literature reviews hence developing related solution on basic security function and countermeasure. Author observes that most the frameworks focus on the software
development cycle and forget to extend to scope to IoT device performance safety and security. The authors propose a generic model to address security which answers question on what, why, how and when on the stages of security and privacy were to be considered on the outer layer. The security challenges of data protection, device boot, monitoring, reporting, authentication and communication were considered in the next inner layer. The privacy challenges for personal data protection by the means of encryption and the protection of the IoT device were considered in the innermost layer. They provide a chart of comparative analysis illustrating the limitation of the existing system and proposed improvements.

2.30 Xiaoquili et. al., (2017), in this paper describe the need and the importance to conduct an examination Bitcoin and Ethereum on the consensus mechanism (PoW, PoS, PBFT, DPoS, POET, PoA) and propagation mechanism in blockchain technology. The blockchain 1.0 was developed for cryptocurrency and blockchain 2.0 was for smart contacts. On describing the working of the above two the authors compare the traditional currency transaction with cryptocurrency characteristics and advantages, this comparison is extended to distributed application (dAPP) used in Blockchain 2.0. On surveying in attacks on popular system. The author further analysis Self Mining, DAO attack, balance attack and other attacks on the blockchain in the paper. Lastly, they summarize security enhancements by implementation of Smart pools for qualitative frameworks, OYENTE for detection of bugs on the Ethereum smart contract, Hawk, Town Crier to blockchain System.

2.31 Zejun Ren et. al., (2017), introduce security and privacy on the fast increasing IoT network of devices with diverse application of it in real life. Since there is no uniform architecture of the IoT the authors observe that there are different attack on different layers. The paper gives a detail table of comparison between all the key technologies at short range with their characteristics of standards, frequencies, range, data rates and maximum nodes handled. The authors observed that the most untouched area was privacy of information between two entities which were vulnerable to attacks as the end devices which were accessible to information were expose to public and malicious attack as the data moved to datacenter. Privacy is composed of respondent privacy, owner privacy, ethics and laws and describe how it is achieved.
2.32 Zbin Zheng et. al., (2017), considers the various blockchain technologies review and list out the challenges on the recent advance in IoT. Summarizing the key characteristic of the blockchain the author gives a taxonomy of the properties and the various block chain ie public, consortium, private. The public block was open to the world and user communities while the consortium blockchain (Hyperledger and Ethereum) were for the business application. The consensus process (Pow, PoS, tendermint) helps in determining if the node can be trusted or not. The author briefly describes algorithms and compares them with properties of the nodes like identity management, energy saving, tolerated power of the adversary. The author describe GHOST (Greedy Harvest – Observed Subtree) to choose a better miner in the higher block generation. For the multiple challenges of scalability, privacy, self-mining the author recommends redesigning of the block chain (Bitcoin -NG), Zero knowledge proof and zero block respectively. The author recommends the developments in the concept of trusting decentralization at BigData analysis and Smart Contracts.

2.33 Ana Reya et.al., (2018), in this paper the author observes that building trust in distributed environments without the need for authorities is a technological advance that has the potential to change many industries, the IoT among them. Distributed technologies such as big data and cloud computing have been leveraged by IoT to overcome its limitations since its conception by blockchain. This paper focuses on integration of IoT in IoT-IoT, IoT to Blockchain and hybrid approach (IoT to Blockchain Via fog ), Then authors investigates challenges of storage, capacity scalability, security, data anomality and privacy, Smart contract, legal issues, consensus algorithm in blockchain IoT applications on integration and surveys the most relevant work in order to analyse how blockchain could potentially improve the IoT.

2.34 Chan Hyeok Lee and Ki-Hyung Kim , (2018), observed that when data or device authentication information is put on a block chain IoT, personal information may be leaked through the proof-of-work process or address search. They suggest that ZeroKnowledge proof to a smart meter system to prove that a prover without disclosing information such as public key, and have studied how to enhance anonymity of block chain for privacy protection. They used the Mobius IoT open server platform to upload or share data from
sensor to the blockchain server. In Ethereum smart contract all users prove themselves valid, increases reliability. provide anonymity in enhanced blockchain maintains privacy and secrecy. The zero-knowledge authentication protocol has two function of registration and authentication which has a public key and the data is stored in the server. The author verifies that the data for the smart meter and the dispose ledger to make data impossible to modify and modulated smart meter ID. Integrity, verification can be checked by the time consumption for mining transactions.

2.35 Daniel Minoli and Benedict Occhiogrosso, (2018) in theirs paper concludes that in IoT environments where Blockchain mechanisms (BCM) play an important role BCMs are only part of the IoT Security (IoTSec) solution. They come to a conclusion from the factor that impact IoT security and challenges associated with reliable security in IoT are driven. They divide the IoT security in lower layer to secure sensor devices and base station/gateway where blockchain is used for sensor data and aggregated data respectively. in the upper layer the PKI and end to end blockchain is used. The author a after describing the block and block chain structure provides over 15 reasons why Blockchain is best to implement security and data integrity. Based on the 7 layers of IoT framework the author charts out the Inlayer security mechanism with the implementation of block chain.

2.36 Jianli Pan et.al., (2018), the authors address the emerging blockchain and smart contracts technologies bring a series of new security features for IoT and edge computing, with design and prototype an edge-IoT framework named “EdgeChain” based on blockchain and smart contracts. They integrate a permissioned blockchain and the internal currency or “coin” system to link the edge cloud resource pool with each IoT device account and resource usage, and hence behavior of the IoT devices. EdgeChain uses a credit-based resource management system. Smart contracts are used to enforce the rules and policies to regulate the IoT device behavior in a non-deniable and automated manner. All the IoT activities and transactions are recorded into blockchain for secure data logging and auditing. They implement an EdgeChain prototype, a testbed and conduct extensive experiments to evaluate the ideas EdgeChain. The results show that while gaining the security benefits of blockchain and smart contracts, the cost of integrating them into EdgeChain is within a
reasonable and acceptable range. The paper offers workflows and result analysis of the prototype.

2.37 Matevz Putisek et. al, (2018) compares the different distributed ledger protocol like Ethereum, Hyperledger fabric and IOTA (which is based on a new block-less distributed ledger architecture) from the IoT application development perspective. The IoT applications based on blockchain (BC) can incorporate the on-chain logic (the smart contracts) and Web, mobile or embedded client front-end application parts. They differed in positioning of Ethereum blockchain clients (local device, remote server) and in positioning of key store needed for the management of outgoing transactions. Practical architectures, used the Ethereum network for trusted transaction exchange, are the data volumes, the location and synchronization of the full blockchain node and the location and the access to the Ethereum key store. In addition, they proposed the use of architectures with a proprietary communication between the IoT device and remote block

2.38 Mohammed Amine et. al., (2018) . The paper describes the blockchain structure with the survey which have been carried out by a set of individuals that finds out contribution of the Bitcoin protocol and application, feasibility in consensus protocol, privacy, application of Blockchain structured IoT. Their study was focused on security and privacy The authors classifies threats models, their countermeasures and resistant Protocol for 16 attacks and studies existing research on security and privacy is based on authentication, privacy and trust to prove the above. The author surveys 16 Blockchain Models their security model, and the results reassure the Blockchain shows résistance to combined attack, it shows dynamic and adaptable security framework as there are several services to be regulated. The block chain is compliance with GDPR and grants end user power over personal data. The blockchain provide energy efficiency consensus algorithms for mining as data grows.

2.39 Pankesh Patil et. al, (2017), in their paper outline an intelligent approach that facilities the automated transition between the edge and the cloud depending in the dynamic condition of the IoT infrastructure and application requirements. Fog computing for data analytics became difficult because of battery life of the device, availability and mobility. Here the Fog node leverages on demand cloud resource and coordination distribution globally and adapt a dynamic approach make the edge intelligent creating FogNets, similar to Mobile edge
computing nets or CloudNets. The Edge framework enables efficient execution of the machine precepts on resources-constrain IoT devices and use bit vector encoding to represent domain knowledge and implement a semantic perception algorithm. It also speeds up the analytics task by parallelism, by segmentation of the tasks and optimization. The fog node prefers analytics locally an send the data to the cloud, while local user localized protocol to provide better service. The author describes the nodes as the edge to play the roles of the surrogate, storage, content manager, petitioner and off loader. Heterogeneity, deployment and programming are the difficulties in implementation of this approach.

2.40 Roshan Doshi et. al., (2018), in their paper describe the vulnerability of the IoT device to DDOS attacks on a critical Internet infrastructure. The author provides a solution of automatically detection and confronting the attack by machine learning. Considering the anomaly behavior detection and middlebox limitation a threat model is designed to observe traffic between the customer and the IoT device. A experimental setup for the collection of data normally and even the DOS attack. The traffic collection is analysed for 5 minutes per device where the attack was device independent. Ona analysis of this procedure that produced a dataset of 461,855 packets 459,565 packets were compromised by malicious packets, 32290 benign packets were there. Five machine learning algorithm were tested on IoT datasets that showed that the test set accuracy was higher than 0.99. the authors believe that there is great potential for the application of deep learning to anomaly detection in IoT networks, especially for detecting attacks that are more subtle than DoS floods.