A Review and Development Methodology of a LightWeight Security Model for IoT-based Smart Devices

Mathuri Gurunathan[1], Moamin A. Mahmoud[2]
College of Computing and Informatics
Universiti Tenaga Nasional
Kajang, Malaysia

***Abstract*—Internet of Things (IoT) turns into another time of the Internet, which contains connected smart objects over the Internet. IoT has numerous applications, for example, smart city, smart home, smart grid and healthcare. In common, the IoT system comprises of heterogeneous devices that deliver then trade endless sums of safety-critical information, also as privacy-sensitive information. Nevertheless, connected devices can give your business a genuine lift, yet anything that is connected to the Internet can be vulnerable to cyberattacks. Most present IoT arrangements rely upon centralized architecture by associating with cloud servers through the Internet. The public cloud is described as computing services publicized by third-party suppliers over the Internet, making them accessible to anybody who needs to use or buy them. This solution gives magnificent flexible calculation and information the executives capacities, as IoT systems are developing increasingly mind-boggling; nonetheless, despite everything, it faces different of security issues. One of the weaknesses is that your information moving in IoT devices by means of public cloud could be in danger, despite the fact that the hacker was not explicitly focusing on you and with the public cloud you have insignificant authority over how rapidly you can grow the cloud. In this case, a secured protocol in IoT is vital to ensure optimum security to the information being traded between connected devices. To overcome the limitation, in this paper, we conduct a comprehensive review on existing security protocols and propose a development methodology of a blockchain-based lightweight security model that provides end to end security. By utilizing lightweight, an authenticated client can get to the information of IoT sensors remotely. The presentation investigation shows that lightweight offers better security, less overheads, and low communication.**

Keywords*—*Lightweight; security mode; IoT; smart devices

I. Introduction

The Internet of Things (IoT) is a grouping of connected devices with the Internet. The selection of IoT-based advancements opens up new doors in different parts of our everyday lives, for example, smart home, smart transportation, and manufacturing [1]. Hence, IoT based applications become necessary things in our everyday life [2]. In a cloud-based IoT condition, the cloud stage is utilized to store the information got from the IoT sensors. Cloud innovations are pointed at provisioning steady and shared computational and storage assets to different clients and applications [3]. Public cloud is described as computing services publicized by third-party providers over the Internet, making them open to anyone who needs to use or get them [3] [4]. They may be free or sold on-demand, empowering customers to pay simply examine for the CPU cycles, the capacity they use or bandwidth [4]. Not at all like private clouds, public clouds can spare companies from the high costs of having to buy. Since certain applications in cloud-based IoT are critical bases, the data gathered and sent by IoT sensors must not be leaked during the user to device communication [5]. Be that as it may, public cloud is an increasingly attractive objective for hackers. Your information could be in danger, despite the fact that the hacker was not explicitly focusing on you. It has restricted adaptability in design and security and it isn't perfect for organizations or clients who utilize sensitive information [6]. In this manner, we require secure verification protocol for cloud-driven IoT-based applications in which a genuine client and an IoT sensor can commonly validate each other for secure communication yet in a recently published paper by Bogdan-Cosmin Chifor et.al [7] proposed a theft safe security scheme utilizing a keep-alive protocol that is executed intermittently and each time the client request a Fido verification via cloud platform. The Fido UAF model gives focal points over traditional verification mechanisms, such as strong authentication and a simplified registration and authentication method [8]. In any case, the Fido protocol too presents a few noteworthy limitations: i) the critical functionality of the Fido protocol regularly works in a customer platform such as a mobile device, which is vulnerable to a variety of attacks as malware and infections, its clients convey unsupervised computer program, and the deployed operating systems may be vulnerable to vulnerabilities; ii) the expense is additionally costly on account of the high foundation and support cost related with unified mists, huge server cultivates and organizing hardware. The sheer sum of communications that drive needs to be taken care of once IoT devices develop to the tens of billions will increment those costs significantly [64] [65]68.

To overcome these limitations, in the recent decade, a blockchain has drawn attention to improving reliability, auditability, security, and secrecy of the Internet of Things (IoT) where billions of gadgets are associated with the Internet to ease everyday life and offer customized services. The blockchain is a kind of appropriated record for keeping up an unchanging and deliberately structured record of value-based information [8]. A blockchain limit as a decentralized database

is overseen by PCs having a place with a peer-to-peer (P2P) network. One of the advantages of blockchain is that it's open. Everyone taking part can see the blocks and the transactions stored in them. This doesn't mean everybody can see the real content of your exchange, such that's ensured by your private key.

Be that as it may, the current blockchain suffers from the main challenge which is overheads and scalability. In an average blockchain execution, all blocks are broadcast to and confirmed by all nodes. The bandwidth and memory which are restricted in the IoT devices and these highlights are wasteful to satisfy the complicated security issues and it prompts critical scalability issues since the broadcast traffic and preparing overheads would increase quadratically with the number of nodes in the network [9]. To accord with this, we require lightweight security schemes to verify the correspondence among taking an interest substance in the IoT condition. Thus, this study attempts to answer two questions (i) what are the existing security protocols that have been developed for IoT devices? And (ii) how a lightweight security model can be developed. To do so, we set the two objectives: (i) to study and analyze existing security protocols used in IoT applications, and ii) to propose a development methodology of a blockchain-based lightweight security model that provides end to end security for cloud-driven IoT-based Smart Devices.

II. Review of IoT-based Security Protocols in Smart Applications

A. What is IoT

The loT or the Internet of Things may be a basic concept of connection between electronic devices such as smart-phones, smart TVs, Tabs, Computers and actuators to the Internet. These devices are connected together in such a way that they will be empowering the user to perform an unused medium of communication between things and things additionally between people and things [1]. Within the world of IoT, everything genuine gets to be virtual, which implies that each individual and thing is locatable and addressable, and could be a readable object on the internet. IoT devices will indeed have "the capacity to sense, communicate, organize and create new data, turning into a necessary piece of the Internet.

The progression of the Internet of Things will revolutionize a number of segments, from smart home, smart city, smart grid and etc. IoT idea can likewise be inferred to make another framework and wide upgrade space for smart homes to pro ide smart, quality and to develop the quality of life. In this paper, we center on IoT based smart home applications. A general smart application of IoT environment is presented in Fig. 1.

B. IoT Applications Involved In Security Issues

Fig. 2 shows a comparison of the IoT applications percentage up to the present. We considered five IoT application spaces that include Smart City, Smart Home, Smart Health, and Smart Grid. Smart city and smart home have the highest portion.

Fig. 3 shows the Number of Security Vulnerabilities in Smart application IoT from 2010 – 2018. The result shows a steep increase in 2017 onward.

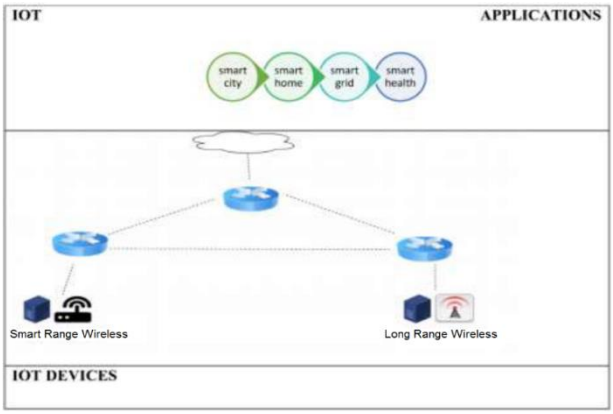

Fig. 1. An Example of IoT Application Environment.

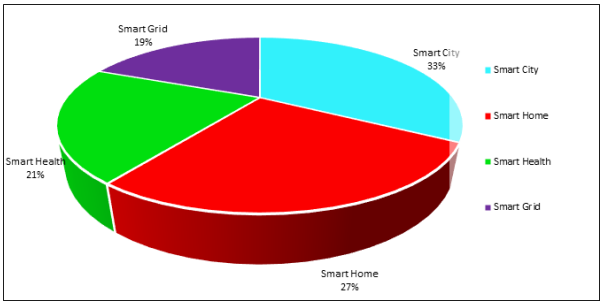

Fig. 2. Percentage of the showed IoT Applications.

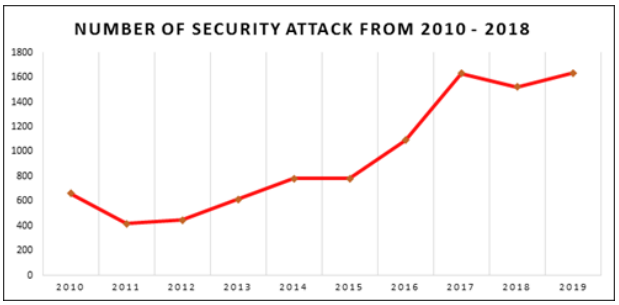

Fig. 3. Number of Security Vulnerabilities in Smart Application IoT.

Fig. 4 presents that the articles on the security protocol of IoT devices in a smart system that were included in this review hailed from 43 nations and nationalities. These articles, for the most part, include a research study conducted within the 43 countries.

In specific, the geological distribution of the picked articles on the security protocol of IoT devices in a smart system as far as numbers and rates show that the premier beneficial authors are from China, with 24 papers. This was taken after by India with 18 papers and USA with 15 study cases; Korea with 14 study cases; Saudi Arabia with 12; France and the Canada with 8 each; Germany, Malaysia, and UK with 6 each; Italy, New York, Pakistan, Singapore and Spain with 5 each; the Australia with 4; Brazil, Poland and Sweden with 3 each; and Indonesia, Japan, Jordon, Romania, Switzerland and Taiwan with 2 each; and Abu Dhabi, Beijing, Beirut Lebanon, Bosnia Herzegovina, Belgium, Egypt, Moscow, Sri Lanka, Thailand, Vietnam and etc. are with 1 paper each. Fig. 2 presented by the authors' nationality.

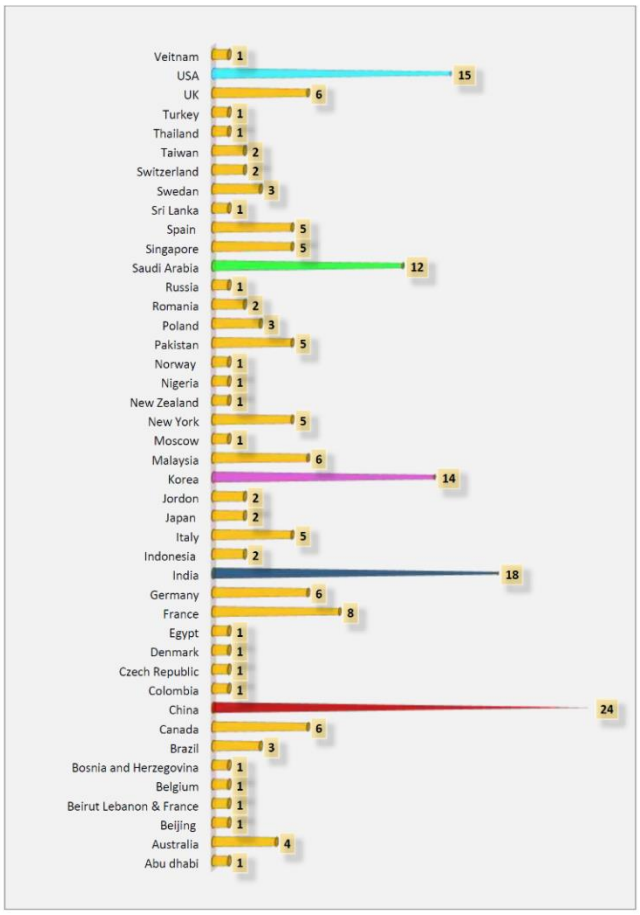

Fig. 4. Distribution by Authors' Nationality.

Smart Home: Smart Home is a term utilized to depict a home that contains a communication network that interfaces with various devices and enables them to be remotely controlled, observed, and got to by utilizing your smartphone applications, PC, and tablets [10]. It allows us to control our home appliances from a remote distance anytime and anywhere with Internet access [7]. The IoT smart home services are growing step by step, the technologies can viably communicate with one another using Internet Protocol (IP) addresses. All smart home devices are associated with the internet in a smart home environment. As the number of devices increases higher inside the smart home environment, the odds of malignant attacks also increase. [11]. One of the premiers touted focal points of a smart home is giving genuine feelings of serenity to house proprietors, empowering them to screen their homes remotely, countering dangers or threats, for example, an overlooked forgotten coffee maker left on or house door left open. In addition, smart home additionally assists consumers with improving capability [12]. Instead of leaving the air conditioning on all day, the home automation system can get familiar along with your behaviors and ensure the house is chilled off once you arrive home from work [13]. Notwithstanding security, various smart home users worry about data privacy. When developing solutions for smart home, security, and privacy are the best concerns [14]. Hence, breaking the security of a home automation system can lead to unauthorized get to access to private information. Existing vulnerabilities like poor setup and the use of default passwords are among the factors that can aid a hacker in compromising at the slightest one device in home automation [15]. Once a single device is compromised, hackers can take several actions based on the capabilities and functions of the device. Subsequently, it is very vital to distinguish all sorts of weaknesses and to address issues that can lead to unauthorized access to management of home automation and their information [16] [68].

Smart City: A Smart city is an urban zone that utilizations different sorts of electronic Internet of things (IoT) sensors to gather data and after that uses of this data to manage resources and resources effectively [17]. The data collected from people, devices and assets that will be processed and analyzed to monitor and manage information, traffic, water supply, hospital, power plants, video monitoring and so on. IoT Technology is making humans life better and easier. One of the ways will be secure wireless connectivity and IoT technology is changing traditional city life [18]-like streetlights into another era intelligent lighting stages with extended capabilities. It incorporates integrating solar power based power and associating with a cloud-based focal control system that will connect to other resources within the environment [19]. However, bringing insecure items into the smart city enormously broadens security and privacy risks. As many devices connected, vulnerabilities in a place get higher where attackers will have many loopholes to get the data [20]. In a general sense, each new device added to an IoT environment includes a new threat to the surface [21].

Smart grid: The smart grid is an electrical grid that is a combination of the electrical network and smart digital communication technology [22]. It has capable of giving electrical control from various and extensively circulated sources, as from wind turbines, solar-oriented control systems, and possibly surely module half and half electric vehicles [23]. A smart grid is a communication network on the beat of the power framework to assemble and analyze information from various parts of a power matrix to foresee power supply also, to predict which can be utilized for power managing [24]. Besides, a smart meter is one of the smart systems from the smart grid. It has installed at many organizations which to monitor the energy conception [25]. Besides, the smart grid has various characteristics such as data rate, time constraints, etc. This will be vulnerable to malicious cyber-attack of varying types that can severely obstruct its far deployment [26].

Smart Health: Smart health is defined by the technology that leads to greater treatment for patients, better diagnostic tools, and devices that can improve the quality of life for every individual. IoT changes the medical information into insights for smarter patient care [27]. Healthcare is now more technologically progressed and is all almost connecting devices together. In this manner, IoT is very important in the health system. Besides, by utilizing devices like connected sensors and other sorts of things that individuals can wear all that data can be placed within the cloud, and the doctor can effectively monitor the real-time data of the patient [28]. Nowadays, numerous healthcare devices operate all through the world which gets to be an issue because it can cause information loss and mistakes in diagnosis. To defeat this the information which

is collected will be stored in the cloud. In security terms, IoT devices have constrained resources and these devices are associated with the internet. Hence, privacy and security are one of the enormous issues with IoT in healthcare [29] [30].

C. Existing Security Protocols

Numerous protocols have been proposed by the literature, Fig. 5 shows the number of security protocols articles from 2010 to 2019 and Fig. 6 shows the top highest number of protocols from 2010 to 2019.

However, in the following sections, we present the most recently used protocols which are, Zigbee, 6LoWPAN, Constrained Application Protocol (CoAP), Software-defined networking (SDN), and Blockchain.

Zigbee: ZigBee is a mesh network protocol. It is outlined to carry small information packets over brief distances whereas keeping up low control consumption. ZigBee is also an open-source wireless technology utilized in low-powered embedded devices (radio frameworks) to encourage productive [31]. It is more like an alternative to Bluetooth and Wi-Fi. ZigBee was based on the IEEE 802.15.4 standard detail and is made by a set of companies that shape the ZigBee Alliance. Whereas other wireless standards are concerned with exchanging huge sums of information, ZigBee is built for devices that have littler throughput needs [32]. Besides, the other driving components are low cost, high reliability, higher security, less battery usage, simplicity and interoperability with other ZigBee devices [33].

Moreover, one of the issues of the wireless sensors is that they require as well much power to operate properly however ZigBee gives long-lasting batteries with which they can remain lively for months or even a long time.

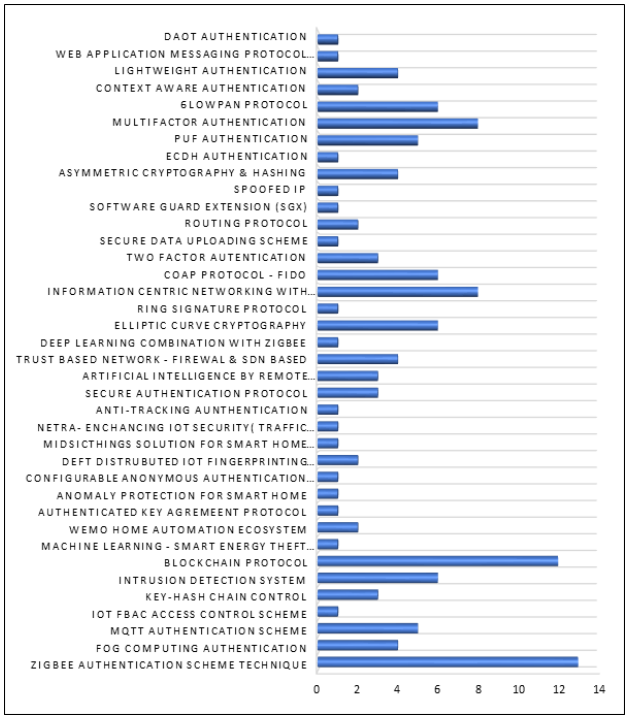

Fig. 5. Number of Security Protocols Articles from 2010 to 2019.

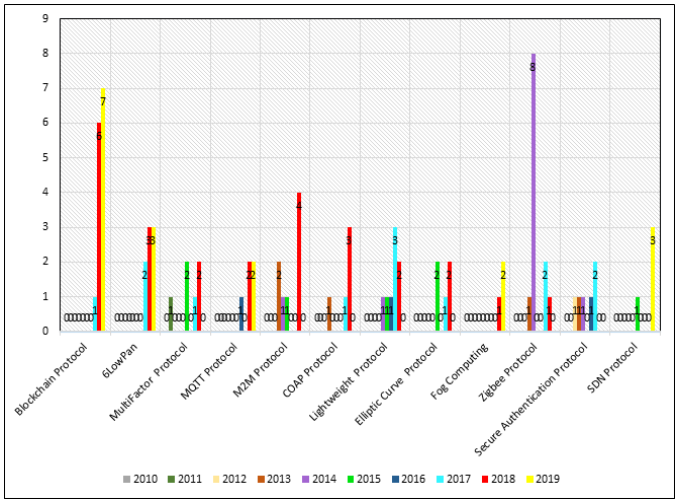

Fig. 6. The Top Highest Number of Protocol from 2010 to 2019.

Likewise, ZigBee devices are a lot less expensive than different devices. The low information rate will play an imperative part in the accomplishment of ZigBee in the future as the organizations will concentrate on the lost cost and low information rate solutions for their issues instead of costly ones [34]. Last but not least, ZigBee's capacity to support mesh networking implies it can boost information transmission extend and give more prominent stability (even when a single connected hub comes up short and doesn't work) but security isn't very well executed by the engineers in ZigBee [35]. The ZigBee network deployment in this study is displayed in Fig. 7.

6LoWPAN: 6LoWPAN is a direct low-cost communication organize that grants wireless network in applications with limited control and loosened up throughput prerequisites as it gives IPv6 organizing over IEEE 802.15.4 frameworks It is molded by devices that are reliable with the IEEE 802.15.4 standard and characterized by brief run, low bit rate, minimal effort, low control, and low memory usage

Exactly when a lower processing capacity sensor node in a 6LoWPAN or purported reduced capacity device (RFD) needs to send its information parcel to an IP-empowered device outside the 6LoWPAN, it at first sends the bundle to the higher preparing ability sensor node or so-called full function device (FFD) in a similar PAN. The FFDs which respond as a switch in 6LoWPAN will advance the information parcel bounce by a jump to the 6LoWPAN entryway. The 6LoWPAN gateway that connects with the 6LoWPAN with the IPv6 domain will at that point forward the packet to the destination IP-empowered device by utilizing the IP address.

A 6LoWPAN system consists of many embedded wireless remote devices that are perceived by the power constraint, low-information rate, and limited memory. The 6LoWPAN architecture is portrayed in Fig. 8 in which the end-to-end communication for interconnecting 6LoWPANs to the Internet is outlined. Each associated 6LoWPAN is an IPv6 stub network on the Internet, on the grounds that the IP packets can be gotten from or sent to it, however, there can't be a packet transit to other Internet systems.

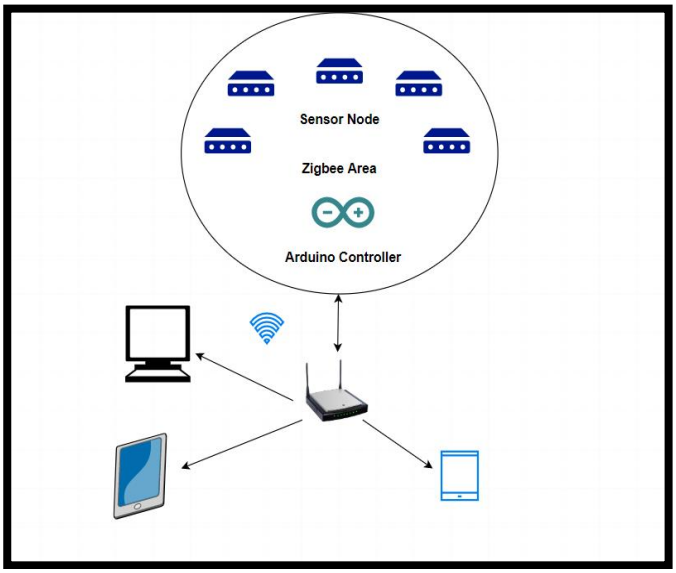

Fig. 7. Zigbee Network.

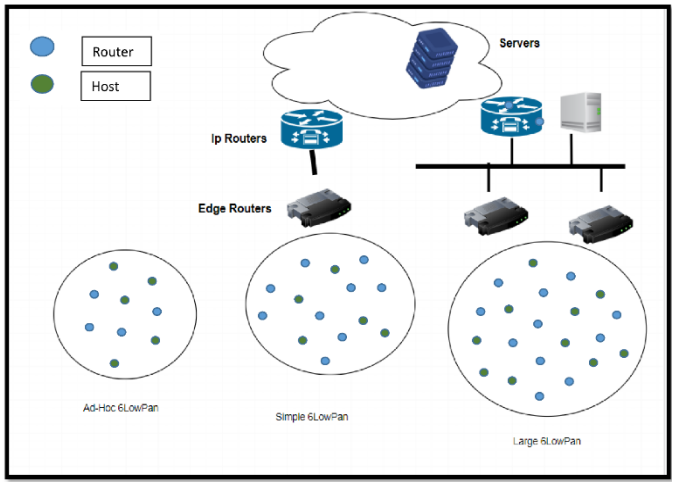

Fig. 8. 6LoWPan Network.

Constrained Application Protocol (CoAP): The Constrained Application Protocol (CoAP) is a web transfer protocol. It has been designed for a constraint environment and by the Internet Engineering Task Force (IETF). The main objective of CoAP is to restrict the required fragmentation by using small message overhead [36]. Also, this protocol appropriate for constrained systems such as 6LoWPAN which underpins the fragmentation of IPv6 packets into little outlines and the examples of the constrained devices is sensors, low power node, switches, and low power networks [37].

Constrained Application Protocol (CoAP) is a simplified version of HTTP and that is because the protocol looks more like a traditional website-based business [38] which gives the capacity to be compatible with an existing network that's web service-based [39]. Besides, this protocol has been created as a specialized web transfer protocol for utilizing constrained nodes and constrained like an example of low-power systems [40]. The CoAP protocol stack, where it utilizes Request/Response and a variant of Publish/Subscribe (Resource/Observe) architectures. The Request/Response model is like the Client/Server model in HTTP. CoAP is proposed to assume a comparable job as HTTP accomplishes for Web Internet and is being considered as a trade of HTTP for IoT networks and is turning into a standard protocol for some IoT solutions.

Software-defined networking (SDN): Software-defined networking (SDN) is a networking worldview that permits consistently centralized control of network switches and routers. SDN permits the probability of making new services and progressively productive applications dependent on the interaction with systems traffic, organize security usage, or quality of service [41]. In SDNs, most of the network capacities are actualized in applications [42]. The SDN controller keeps up a logical outline of the network and covers up the network complexity from applications through reflections.

SDN is a rising and promising innovation to make it occur. SDN decouples the control plane from the information plane. An SDN controller can take contributions from end structures applications and settle on choices to the information plane roughly what traffic can experience [43]. SDN can possibly benefit the security of IoT frameworks in at scarcest three viewpoints. In the first place, it can help shape a feedback-control loop from end IoT frameworks to the SDN controller which helps controls at least one programmable switches. Second, similar attacks to different exploited victims from a similar source inside a similar framework can be blocked and subsequently advantage the total IoT network in a cooperative manner [44]. Lastly, the attacking data can be shared among numerous peering controllers that oversee and control distinctive systems. As shown in Fig. 9, fruitful integration depended on the IoT system's utilization of key SDN highlights [12].

Blockchain: A blockchain is characterized as a distributed database that keeps up a changeless and tamper-proof record of value-based information. A blockchain is totally decentralized by depending on a peer-to-peer arrangement. More absolutely, each note of the arrangement keeps up a copy of the record to avoid a single point of failure. All duplicates are updated and approved at the same time. A block is an information structure that permits Blockchain to record the produced and traded exchanges and each block is connected to the chain by cryptography [45] The Blockchain is a distributed ledger that has three essential attributes: decentralized, transparent and recorded. All members keep and update a duplicate of a distributed ledger to check and approve transaction which makes Blockchain transparent and difficult to hack or lost any information [20]. Every transaction incorporates three principle segments, i.e., the information, the hash, and the hash of the previous block [21]. Each block in the system records the hash of the previous block. This prompts a chain of blocks with improved security. For instance, in Fig. 1, there is a chain of three blocks. Block 3 to block 2 and block 2 points to block 1 utilizing the hashes of previous block 1. On the off chance that hackers alter the second block information, the related block hashes changes. This makes the third block and every ensuing block invalid since they have not put away a legitimate hash of the previous block [21]. In Fig. 10, it presented how blockchain hash generally works.

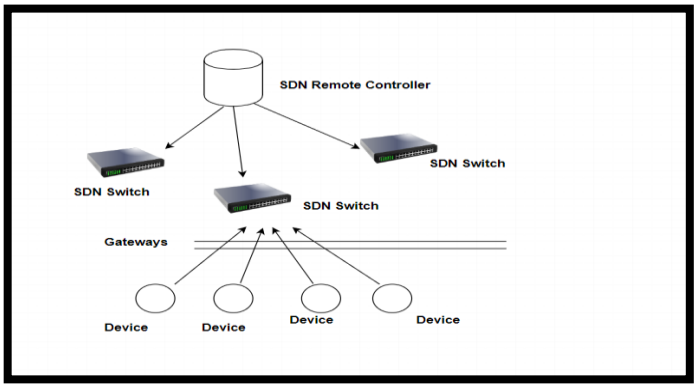

Fig. 9. SDN Network.

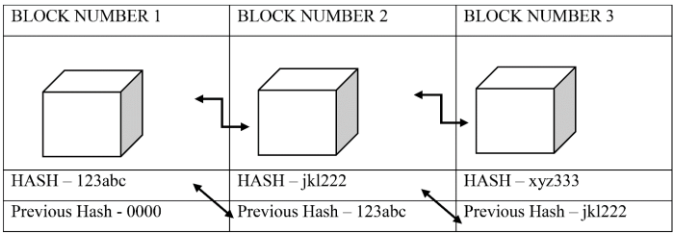

Fig. 10. How Blockchain Hash Works.

III. Why Blockchain Technology

A Blockchain is described as an "advanced, decentralized, and flowed record in which trades are logged and included sequential requests with the objective of making never-ending and tamperproof records" [46]. Basically, it is a novel instrument for storing, sharing information and securing between various nodes in a system [47]. Blockchain parts from the traditional unified by overseeing chain data over a dispersed and interlinked arrangement of nodes. The principle qualities of Blockchains are shared immutability, decentralization, recordkeeping, tamper evidence, distributed trust and tamper resistance [48]. The term 'Blockchain' picked up its prominence as the yield of a combination of configured advancement, methods and tools underpinning the digital currency Bitcoin. In itself, Bitcoin is a decentralized digital currency depending on an open system of a computer system and online communication protocols [49] and was the principal fruitful application based on an online Blockchain.

Using distributed technologies for IoT devices can understand security issues as well as include new features and lessen working expenses [66] [67]. Blockchain is an innovation that works with exchanges and gives communication in the system. It is incredible for monitoring processes in IoT. For instance, in light of the blockchain, you can bolster the identification and disclosure of gadgets, encourage microtransaction exchanges among them, and give proof of payment. In any case, blockchain technology stands to cause an immense effect on the Internet of Things. The blend of information that can't be adjusted however can be followed and verified from connected devices will drive the birth of exchanges among connected devices. With the intensity of blockchain technology, devices will have the option to network and direct trade as microtransactions utilizing a digital currency [50]. Blockchain technology will likewise upgrade security among the connected devices.

Blockchain technology can be utilized in following billions of connected devices, enable the handling of trades and coordination between devices; think about immense hold assets to IoT industry makers. This decentralized methodology would wipe out single points of failure, making a stronger ecosystem system for devices to run on. The record is tamper-proof and cannot be controlled by noxious actors since it doesn't exist in any single area, and what's more, man-in-the-middle attacks can't be organized since there's no single string of communication that can be catching [51]. In an IoT system, the blockchain can keep a changeless record of the historical backdrop of smart devices. This include empowers the independent functioning of smart devices without the required for centralized specialist. Fig. 11 shows the advantages of blockchain.

The perspective on general security requirements just as necessities of security is given by blockchain. Fig. 12 presented the security requirement of blockchain and the following shows a detailed explanation of the security requirement of blockchain.

- Integrity: The point of the integrity of information is to keep up the consistency and accuracy of information all through the lifecycle of information [52].
- Authentication: Authentication is stated to a procedure inside which the credentials gave to get to a file are compared and the ones that are given in the database by the approved clients [53].
- Verifiable: Verifiable substances in the system are important to ensure the blockchain ledger against tampering [54].
- Confidentiality: Confidentiality of information is to protect it from unveiling to unauthorized parties [55],
- Trust: The fundamental job of producing trust is to guaranteeing trustworthiness, reliability or the capability of the individual system nodes based on the applied monitoring schemas [56] [57].
- Anonymity: Anonymity has applied consequently with the execution of the blockchain. In the blockchain, exchanges are performed with secret keys and the public [58].
- Immutability: Traditional relational databases give variable storage, as changes made to a particular record or table are supplanted in that document [59].
- Authorization: the authorization is a procedure wherein the get to a level of a previously authenticated client is allowed. In which it is resolved that activities can a client performed and for what he/she isn't permitted [60].
- Privacy: The blockchain-based IoT approaches in the writing who have kept up the privacy are [54] [61].

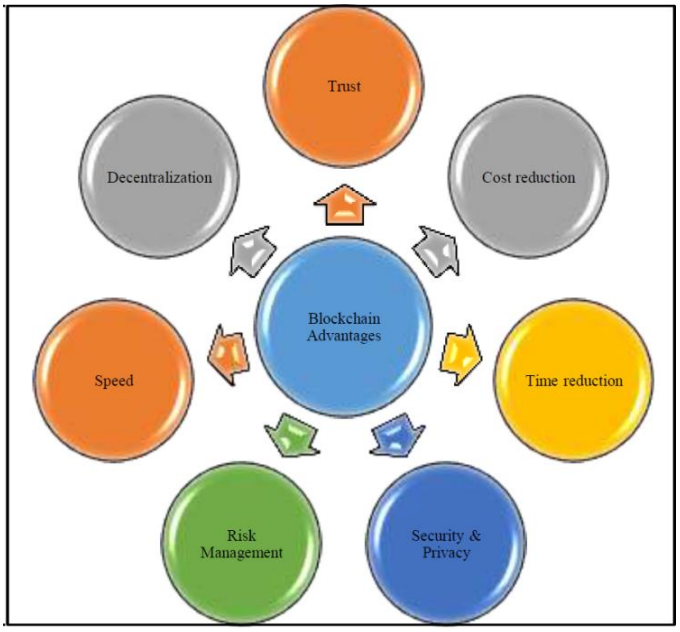

Fig. 11. The Advantages of Blockchain.

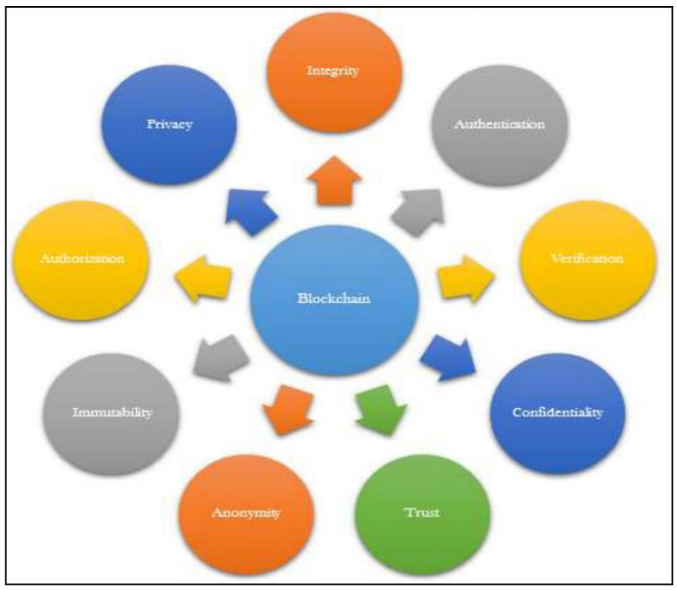

Fig. 12. Presented Security Requirement of Blockchain.

IV. Development Methodology

In research design, we conceive a collection of research activities that lead to the achievement of the research objectives. Fig. 13 shows the research activities that we compiled as the research design. It consists of activities that review the literature to develop the problem statement along with the research questions and objectives. Particularly, the study relies on the existing models in the literature to develop the conceptual model. The models are efficient Lightweight integrated Blockchain (ELIB) which is our baseline method; A Lightweight Scalable Blockchain (LSB), and a Universal Authentication System Protocol (UAF-FIDO).

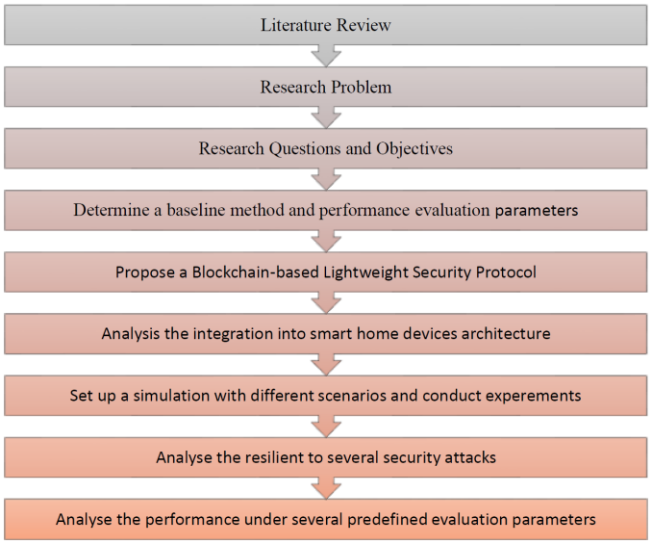

Fig. 13. Development Methodology of a Blockchain-based Light Weight.

A. Determine a Baseline Method and Performance Evaluation Parameters

The efficient Lightweight integrated Blockchain (ELIB) model is created to meet the requirements of secure IoT. The ELIB accomplishes a sum of half sparing (50%) in dealing with time on contrasting with the baseline method with the base energy utilization. The experiment exhibited that the ELIB shows the most extraordinary performance under a couple of evaluation parameters.

The ELIB models need more time for packet handling with when just like the baseline which has the component of the extra-encryption and hashing limits. Within the destitute case for the inquiry-based store T, additional overhead brought about by ELIB that is incredibly low in absolute terms.

B. Propose a Blockchain-Based Lightweight Security Protocol

In spite of the fact that Blockchain is a viable technology for giving privacy and security in IoT, applications within the IoT context presents a few noteworthy challenges. IoT devices don't have adequate memory, control, for calculating or zone for executing a hardware module, since the device can perform a particular reason. Therefore, we use lightweight to overcome the restriction. Within the architecture of the smart home, we supplant fido protocol and integrate with blockchain-based lightweight to decrease packet overheads on IoT devices and to have secure communication with clients and gadgets. Consequently, IoT devices have constrained resources, hence, confirming all modern blocks and exchanges may be distant past their capabilities. To guarantee scalability and lessen processing and packet overhead on IoT devices, we accept that the blockchain is overseen by a subset of the overlay hubs. This decreases the packet overhead for information transactions. To guarantee information integrity, the exchange corresponding to the traded information between overlay nodes contains the hash of the information signed by the exchange generator [9].

C. Analysis of the Integration into Smart Home Devices Architecture

Within the architecture of the smart home, we supplant fido protocol and integrate with blockchain-based lightweight to diminish parcel overheads on IoT gadgets and to have secure communication with clients and devices. Consequently, IoT devices have restricted assets, in this way, confirming all modern blocks and exchanges may be distant past their capabilities. To ensure scalability and lessen handling and packet overhead on IoT devices, we acknowledge that the blockchain is overseen by a subset of the overlay nodes. Here, each person node within the overlay is called as PK. This decreases the packet overhead for information trade. To guarantee information integrity, the transaction compared to the exchanged information among overlay nodes contains the hash of the information signed by the exchange generator.

D. Set up a Simulation with different Scenarios and Conduct Experiment

Here we utilize two simulators as takes after to evaluate the performances of the proposed solution and Table I shows a brief summary of the simulator.

E. Analyze the Resilient to Several Security Attacks

The study comes up with several security attacks to which IoT systems or blockchains are especially vulnerable and layout how LSB secures against them.

Denial of Service (DOS) attack: The design of DOS attack has a few hierarchical security protection against this attack. It has few levels of a protective layer that can be credited to the reality that it would be impossible for an attacker to straightforwardly install malware on smart IoT devices since these devices are not legitimately accessible [62]. Let us for a minute expect that the attacker some way or another still figure out way of how to infect the devices. There it comes the LSB which is Lightweight Scalable Blockchain ensures against these attacks. The method of LSB is to defend the attack like the example of OBM. Overlay Block Manager (OBM) would not send an exchange to their cluster members except if they discover a match with a substance in their key list.

Dropping attack: The attacks influence the consumption of energy and packet drop parameters in the network [63]. From the attack, OBM is an entity responsible for the blockchain management. Therefore, OBM drops exchanges to or on the other hand from its cluster members to confine them from the overlay network. A segment of the exchanges is verified as the OBMs manufacture up trust in each other. To ensure along with the attack, a cluster member can change the OBM it is related to on the off chance that it sees that its exchanges are most certainly not being handled.

TABLE. I. SIMULATOR BRIEF EXPLANATION

Tool	Description
Cooja Simulator	Utilize Cooja to consider the performance of the smart home tier.
NS3 Network Simulator	Utilize NS3 to evaluate the overlay performance because it has been broadly utilized for analyzing peer-to-peer systems

Blockchain: If an attacker advertises a false record of blocks and makes it as the longest record. The proposed DTC will restraint the number of blocks each OBM can create in a time interval. This will constrain the number of noxious blocks that an OBM can affix.

F. Analyze the Performance under Several Predefined Evaluation Parameters

This phase gives a point by point validation of a distinctive view of the proposed protocol. To assess the performance, four evaluation parameters have been identified from the literature, processing time, energy usage, overhead, and Scalability.

V. CONCLUSION

Security is consistently and will be a critical perspective on the IoT network. In this paper, it has indicated how the security concerns in the IoT applications have developed. The methodical mapping process of this study discovers how the development has occurred, what sorts of concerns and solutions exist, and what gaps remain. Based on the review outcomes, the public cloud that shares computing services among different customers runs by third-party suppliers over the Internet, making devices accessible online. However, the public cloud is an increasingly attractive objective for hacker and information in the cloud is risky. Therefore, reliable protocol to securely communicate between IoT devices and the cloud is inevitable. On the other hand, Blockchain Can Be Game-Changer for IoT for now and the future. Despite the advantages of blockchain technology, several limitations have been addressed in this study such as High Complexity, Restricted Scalability, High Bandwidth Overhead, and Latency –Delay & overhead. To overcome these limitations, in our future work, we shall develop a lightweight security scheme to verify the correspondence among taking an interest substance in the IoT condition. More specifically, we shall propose a blockchain-based lightweight solution that offers better security and low communication.

ACKNOWLEDGMENT

This project is sponsored by Universiti Tenaga Nasional (UNITEN) under the Bold Research Grant Scheme No. 10346494/B/2019046.

REFERENCES

[1] Ahmad, S., Hang, L., & Kim, D. H. (2018). Design and implementation of cloud-centric configuration repository for DIY IoT applications. Sensors, 18 (2), 474.

[2] Höller J., “Introduction to a New Age of Intelligence,” Mach. to Internet Things, 2014.

[3] Sriram D., “Trust Based Security for Cloud Systems What needs to be done to solve this problem ? What has been done ? What can be done ?,” pp. 3–5.

[4] Delsing, J., Eliasson, J., van Deventer, J., Derhamy, H., & Varga, P. (2016, December). Enabling IoT automation using local clouds. In 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT) (pp. 502-507). IEEE.

[5] Wazid, Mohammad, et al. "LAM-CIoT: Lightweight authentication mechanism in cloud-based IoT environment." Journal of Network and Computer Applications 150 (2020): 102496.

[6] Eric Vanderburg, “Public Cloud Security Concerns Remain after Recent Study,” TCDI Blog, 2019.

[7] Chifor, B. C., Bica, I., Patriciu, V. V., & Pop, F. (2018). A security authorization scheme for smart home Internet of Things devices. Future Generation Computer Systems, 86, 740-749.

[8] Cooijmans, T., de Ruiter, J., & Poll, E. (2014, November). Analysis of secure key storage solutions on android. In Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones & Mobile Devices (pp. 11-20).

[9] Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Lsb: A lightweight scalable blockchain for iot security and privacy. arXiv preprint arXiv:1712.02969.

[10] Marikyan, D., Papagiannidis, S., & Alamanos, E. (2019). A systematic review of the smart home literature: A user perspective. Technological Forecasting and Social Change, 138, 139-154.

[11] Yoon, S., Park, H., & Yoo, H. S. (2015). Security issues on smarthome in IoT environment. In Computer science and its applications (pp. 691-696). Springer, Berlin, Heidelberg.

[12] Jacobsson, A., Boldt, M., & Carlsson, B. (2016). A risk analysis of a smart home automation system. Future Generation Computer Systems, 56, 719-733.

[13] Lyu, Q., Zheng, N., Liu, H., Gao, C., Chen, S., & Liu, J. (2019). Remotely Access "My" Smart Home in Private: An Anti-Tracking Authentication and Key Agreement Scheme. IEEE Access, 7, 41835-41851.

[14] Schiefer, M. (2015, May). Smart home definition and security threats. In 2015 ninth international conference on IT security incident management & IT forensics (pp. 114-118). IEEE.

[15] Mohammad Z., Qattam T. A., and Saleh K., "Security Weaknesses and Attacks on the Internet of Things Applications," 2019 IEEE Jordan Int. Jt. Conf. Electr. Eng. Inf. Technol., pp. 431–436, 2019.

[16] Lin B. N. H, "IoT privacy and security challenges for smart home environments." 2016.

[17] Kumar A., Zeadally S., and He D., "Taxonomy and analysis of security protocols for Internet of Things," Futur. Gener. Comput. Syst., vol. 89, pp. 110–125, 2018.

[18] Airehrour D., Gutierrez J., and Kumar S., "Journal of Network and Computer Applications Secure routing for internet of things : A survey," vol. 66, pp. 198–213, 2016.

[19] Gemalto, "Secure, sustainable smart cities and the IoT," 2019. [Online]. Available: https://www.gemalto.com/iot/inspired/smart-cities.

[20] Ribagorda A., Alcaide A., and Palomar E., "Anonymous authentication for privacy-preserving IoT target-driven applications," vol. 7, 2013.

[21] El-hajj M., Fadlallah A., and Serhrouchni A., "Taxonomy of Authentication Techniques in Internet of Things (IoT)," 2017.

[22] Antonopoulos A. M., "Mastering Bitcoin: unlocking digital cryptocurrencies," O'Reilly Media, Inc., vol. 6, no. 5, pp. 900–917, 2014.

[23] Miloslavskaya N. and Tolstoy A., "Internet of Things : information security challenges and solutions," Cluster Comput., vol. 22, no. 1, pp. 103–119, 2020.

[24] Ghasempour, "Optimum Number of Aggregators based on Power Consumption, Cost, and Network Lifetime in Advanced Metering Infrastructure Architecture for Smart Grid Internet of Things.," Proc. IEEE Consum. Commun. Netw. Conf. (IEEE CCNC 2016), p. 2016, 2016.

[25] Sheik Dawood M. J. M. M., Abinaya P, "Improving the Network Lifetime and Energy Conservation using Target Trail in Cluster of Mobile Sensor Networks," Asian J. Res. Soc. Sci. Humanit., no. 18, pp. 430–447, 2016.

[26] Gupta V. A. B. B., "Security in Internet of Things : issues , challenges , taxonomy , and architecture," Telecommun. Syst., vol. 67, no. 3, pp. 423–441, 2018.

[27] Jing Q., A. Vasilakos V, and Wan J., "Security of the Internet of Things : perspectives and challenges," pp. 2481–2501, 2014.

[28] Neelam S., "Internet of Things in Healthcare," Computing at Blekinge Institute of Technology, 2017.

[29] Madakam S. T. S., Ramaswamy R., "Internet of Things (IoT): A literature review," J. Comput. Commun., p. 164, 2015.

[30] Suresh R. A. P., Daniel J. V., Parthasarathy V., "A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment," Sci. Eng. Manag. Res. (ICSEMR), 2014 Int. Conf. on, 2014, pp. 1–8, 2014.

[31] Yiqi W., Lili H., Chengquan H., Yan G., and Zhangwei Z., "2014 Fifth International Conference on Intelligent Systems Design and Engineering Applications A ZigBee-based smart home monitoring system," 2014 Fifth Int. Conf. Intell. Syst. Des. Eng. Appl., pp. 114–117, 2014.

[32] Gao L., Wang Z., Zhou J., and Zhang C., "Design of Smart Home System Based on ZigBee Technology and R & D for Application," no. January, pp. 13–22, 2016.

[33] Lewis E., Cook F. L. D. J. and Das S. K., "Wireless Sensor Networks," in Smart Environments: Technologies, Protocols and Applications," no. January, pp. 227–228, 2014.

[34] Talal M., "Smart Home-based IoT for Real-time and Secure Remote Health Monitoring of Triage and Priority System using Body Sensors : Multi-driven Systematic Review," 2019.

[35] Kulkarni S., "Considering Security For ZigBee Protocol Using Message Authentication Code," no. February, 2019.

[36] AliA. A. and Member H. I. S., "Constrained Application Protocol (CoAP) for the IoT," no. May, 2018.

[37] Randhawa R. H., Hameed A., and Mian A. N., "Energy efficient cross-layer approach for object security of CoAP for IoT devices," Ad Hoc Networks, no. xxxx, p. 101761, 2019.

[38] Lamichhane M., "CoAP for IOT," ITMO University, Russia, 2017.

[39] Jonathan Fries, "Why are IoT developers confused by MQTT and CoAP," 2017. [Online]. Available: techtarget.com.

[40] Jang S., Lim D., and Kang J., "An Efficient Device Authentication Protocol Without Certification Authority for Internet of Things," Wirel. Pers. Commun., vol. 91, no. 4, pp. 1681–1695, 2016.

[41] Olivier F., Carlos G., and Florent N., "New Security Architecture for IoT Network," Procedia - Procedia Comput. Sci., vol. 52, no. BigD2M, pp. 1028–1033, 2015.

[42] Open Network Foundation, "Software-Defined Networking: The New Norm for Networks.," 2017. [Online]. Available: https://www.opennetworking.org/images/stories/downloads/ sdn-resources/white-papers/wp-sdn-newnorm.pdf.

[43] Sharma P. K., J. Park H., Jeong Y., and Park J. H., "SHSec : SDN based Secure Smart Home Network Architecture for Internet of Things," pp. 913–924, 2019.

[44] Ahmed A. W., "Software Defined Network (SDN) Based Internet of Things (IoT): A Road Ahead," no. July, 2017.

[45] Wüst K. and Gervais A., "›'Do you need a blockchain?,'" Crypto Val. Conf. Blockchain Technol. (CVCBT). IEEE, 2018, pp. 44–45, 2018.

[46] Treiblmaier H., "The impact of the blockchain on the supply chain: a theory-based research framework and a call for action," Supply Chain Manag., vol. 23, no. 6, pp. 545–559, 2018.

[47] Atlam H. F. and Wills G. B., Intersections between IoT and distributed ledger, 1st ed., vol. 115, no. January. Elsevier Inc., 2019.

[48] Rauchs M. et al., "Distributed Ledger Technology Systems: A Conceptual Framework," SSRN Electron. J., no. August, 2018.

[49] Fosso W. S., Kala Kamdjoug J. R., Epie Bawack R., and Keogh J. G., "Bitcoin, Blockchain, and FinTech: A Systematic Review and Case Studies in the Supply Chain Blockchain, and FinTech: A Systematic Review and Case Studies in the Supply Chain. Production Planning and Control, Forthcoming. *Corresponding author Bitcoin, Bloc," pp. 0–53, 2018.

[50] Zhang A., Zhong R. Y., Farooque M., Kang K., and Venkatesh V. G., "Blockchain-based life cycle assessment: An implementation framework and system architecture," Resour. Conserv. Recycl., vol. 152, no. May 2019, p. 104512, 2020.

[51] Treiblmaier H., "Toward More Rigorous Blockchain Research: Recommendations for Writing Blockchain Case Studies," Front. Blockchain, vol. 2, no. May, pp. 1–15, 2019.

[52] Apte S. and Petrovsky N., "Will blockchain technology revolutionize excipient supply chain management?," J. Excipients Food Chem., vol. 7, no. 3, pp. 76–78, 2016.

[53] Patil H. K. and Seshadri R., "Big data security and privacy issues in healthcare," Proc. - 2014 IEEE Int. Congr. Big Data, BigData Congr. 2014, pp. 762–765, 2014.

[54] Zhang J., "A multi-transaction mode consortium blockchain," Int. J. Performability Eng., vol. 14, no. 4, pp. 765–784, 2018.

[55] Hersh W. R. et al., "Health Information Dissemination from Hospital To Community Care : Current State And Next Steps In Ontario," J. Med. Syst., vol. 63, no. 50, pp. 425–432, 2016.

[56] Sun Y., Han Z., and K. Liu J. R., "Defense of trust management vulnerabilities in distributed networks," IEEE Commun. Mag., vol. 46, no. 2, pp. 112–119, 2008.

[57] Entrust, "The Concept of Trust in Network Security," Entrust White Pap., no. August, pp. 1–7, 2000.

[58] Hodges E., "Blockchain is where anonymity meets transparency," 2018.

[59] Morrison A., "The rise of immutable data stores," 2018. [Online]. Available: http://usblogs.pwc.com/emerging-technology/the-riseof-immutable-data-stores/.

[60] Biswas K. and Muthukkumarasamy V., "Securing smart cities using blockchain technology," Proc. - 18th IEEE Int. Conf. High Perform. Comput. Commun. 14th IEEE Int. Conf. Smart City 2nd IEEE Int. Conf. Data Sci. Syst. HPCC/SmartCity/DSS 2016, no. December, pp. 1392–1393, 2017.

[61] Kravitz J. C. D.W., "Securing user identity and transactions symbiotically: IoT meets blockchain," Glob. Internet Things Summit, GIoTS, 2017.

[62] Dorri A., Kanhere S. S., Jurdak R., and Gauravaram P., "Blockchain for IoT security and privacy: The case study of a smart home," 2017 IEEE Int. Conf. Pervasive Comput. Commun. Work. PerCom Work. 2017, no. October, pp. 618–623, 2017.

[63] Eastman D. and Kumar S. A. P., "A simulation study to detect attacks on internet of things," Proc. - 2017 IEEE 15th Int. Conf. Dependable, Auton. Secur. Comput. 2017 IEEE 15th Int. Conf. Pervasive Intell. Comput. 2017 IEEE 3rd Int. Conf. Big Data Intell. Comput. 2017 IEEE Cyber Sci. Technol. Congr. DASC-PICom-DataCom-CyberSciTec 2017, vol. 2018-January, pp. 645–650, 2018.

[64] Al-Momani, A. M., Mahmoud, M. A., & Ahmad, M. S. (2018). Factors that influence the acceptance of internet of things services by customers of telecommunication companies in Jordan. Journal of Organizational and End User Computing (JOEUC), 30(4), 51-63.

[65] Al-Momani, A. M., Mahmoud, M. A., & Ahmad, M. S. (2019). A review of factors influencing customer acceptance of internet of things services. International Journal of Information Systems in the Service Sector (IJISSS), 11(1), 54-67.

[66] Al-Momani, A. M., Mahmoud, M. A., & Ahmad, M. S. (2018). Identification of Factors Influencing Customer Acceptance and Use of IoT Services. Advanced Science Letters, 24(10), 7428-7432.

[67] Al-Momani, A. M., Mahmoud, M. A., & Ahmad, M. S. (2016). Modeling the adoption of internet of things services: A conceptual framework. International Journal of Applied Research, 2(5), 361-367.

[68] Kumar, K., & Mahmoud, M. A. (2017). Monitoring and Controlling Tap Water Flow at Homes Using Android Mobile Application. American Journal of Software Engineering and Applications, 6(6), 128-136.