Efficiency of IoT technology and Associated Technologies in Research

Javad Shahrabi Farahani[a], **Hamed Ahmadi**[b*], **Alireza rivaz**[c]

[a]M.C.A, Computer Engineering Department, Islamic Azad University,Yadegar Emam, Tehran, Iran, Email: Jfarahani361@gmail.com
[b*] M.C.A, Computer Engineering Department, Islamic Azad University,Yadegar Emam, Tehran, Iran, Alirezarivaz@yahoo.com
[c] P.H.D, Computer Engineering, Islamic Azad University,Yadegar Emam, Tehran, Iran, Ahmadihd@gmail.com,

Article History: Received: 14 July 2020; Accepted: 2 January 2021; Published online: 5 February 2021

Abstract: The Internet of Things' fundamental goal is to enable the automated flow of data between two systems or devices without the need for human intervention. Certain communication protocols enable this automated information sharing between two devices. The goal of this research is to determine how effective IoT technologies are in research. The descriptive-analytical research approach was used, as well as the utilization of library resources. The use of undefined networks (SDN) and increasing IoT quality indicators using SE2 and SP2 techniques, utilizing a security framework based on evolutionary algorithms to increase IoT security, and leveraging blockchain in IoT, as well as LPWAN technologies, were all investigated in this study. SP2 enhances the performance of controller plates, which can minimize service latency in spectral computing, according to the findings. By changing the number of transfers in each VM independently, SE2 may give different functionality between control panels. The encryption and decryption processes employ genetic algorithm (interaction and mutation) operations, and GA (interaction and mutation) procedures are applied to each pair of blocks to aid the IoT function.

Keywords: IoT, Genetic algorithm, LPWAN technology, SDN networks

Introduction

Many of the things and gadgets around us that are connected to the Internet and can be controlled and managed by programs on smartphones and tablets are referred to as the Internet of Things. Kevin Ashton invented the term "internet of things" in 1999. In the realm of entrepreneurship, IoT technology is quite essential. Numerous businesses have been founded on the basis of this technology, despite the fact that both the concept and the technology are still in their early stages, with fresh modifications and advances occurring on a daily basis. For Iranian entrepreneurs and creative researchers, using this technology is a great opportunity that may assist enhance the country's economic climate and employment development (Safari, 2015). The Internet of Things' fundamental goal is to enable the automated flow of data between two systems or devices without the need for human intervention. Some specialized communication protocols enable this automated information sharing between two devices (Sen, 2013).

Because IoT nodes have limited battery life, performing computations and transfers while minimizing power consumption is difficult. Indeed, processing one bit of data uses more energy than processing another bit of data. The battery life of the nodes has a significant impact on their lifetime. Depending on the application, IoT nodes are often densely placed in the field of interest, impacting the performance of a routing protocol. Deployment might be either predetermined or self-organized. If certain, the network nodes are manually configured, and the detected data is sent along predetermined pathways. Network nodes are randomly dispersed in self-organizing systems to produce a perceived topology. A node = can have varied mappings or capabilities according on the application, such as sending, measuring, and aggregating all of these duties precisely in the same node, which quickly consumes the node's energy. The node's varied capabilities compound the challenges connected with data routing and make it even more difficult. Due to the fact that network nodes create redundant and duplicate data, headers or base stations may receive similar packets from numerous nodes, which must be aggregated before being transmitted to the base station. Data can also be collected using signal processing technologies.

Data loss, data corruption, transmitting and receiving incorrect information, data failure, and other system faults and vulnerabilities are all examples of IoT security. It's difficult to establish security in the internet of things. It's tough and large since the Internet platform is the most vulnerable component in the Internet of Things. Objects in the Internet of Things are separated into three categories: objects and hardware, communication channels, and cloud. Users generally have access to objects. There is also a platform for communication between users and the server, as well as cloud storage for the server. It also makes troubleshooting equipment more complicated and time-consuming, as well as causing greater resource damage. The speed and quality of the Internet, as well as the weather, have a direct impact on the usage of items in IoT. Sanctions on Iran, for example, have had a significant impact on this aspect. The effectiveness of IoT-related technologies and technologies is explored in this study.

Theoretical foundations

1. Improvement of IoT quality indicators utilizing SE2 and SP2 techniques and the use of undefined networks (SDN).

1-1-SDN network

The name SDN was developed in recent years, although the concept of user management on sending and receiving has been present in nodes since 1996. Two elements are required to bring the SDN concept to life. First, all switches, routers, and other network equipment must have the same logic design; second, a secure protocol between SDN and network equipment is necessary (Hakiri et al., 2017; Moreno-Vozmediano et al., 2017). Control and data are the two elements of a sdn (Yi et al., 2015). There are two components to the control section: sdn controller and controller and application control. Separation and abstraction are the tasks of the cdn controller component, which provides crucial functions for applications. Application control also gets data and services from the controller and makes decisions in real time. Determines which instructions should be executed. New optimization approaches for Linux have been presented in order to offer abstraction and high performance for SDN control. The first is separate run environment (SE2), which divides the run environment amongst several controllers, and the second is separate closed processing (SP2), which simplifies the Linux network stack. The degree of separation and improvement in performance is determined by the operating system. Has been put into action (Yu et al., 2017). To increase speed, a separate execution environment (SE2) and separate packet processing (SP2) were employed. We may benefit from characteristics like abstraction, optimum use of system resources, and comprehensive APIs when we employ SE2 and SP2 (Lee et al., 2018). The performance of the IoT systems utilized in these SDNs may be improved by optimizing SDNs. SP2 increases the performance of controller plates, which can help minimize spectral computing service latency (Thimmaraju et al., 2018).

2-1-SE2 separate executable environment

SE2 is being developed as a standalone executable environment for controlling pages via VM extraction. When opposed to the extraction procedure, VM extraction provides a distinct operating environment since each VM travels inside its own field of security hardware, resulting in a strong isolation between VMs. VM Extraction divides each control panel's memory area and assigns each VM its own memory address. VM Extraction divides each control panel's memory area and assigns each VM its own memory address. Other controller pages or external users cannot access the real memory address of each controller page in VM extraction. However, utilizing a hidden page or hardware assistance, the physical address of the controller level in VM extraction must be translated into the language of the real device address. As a result, identifying the physical address in VM extraction without the aid of the primary protector is challenging (Lee et al., 2018). When the control panel A substitute crashes owing to erroneous control packets, the control network of the substitute B should be unaffected. One advantage of utilizing virtual machines is that they are maintained by a primary protector, and if the primary protector is trustworthy, VM extraction control panels may be secured against malicious assaults. Furthermore, data on Common Vulnerabilities (CVEs) reveal that Xen, an open source representation of the primary guardian, has a significantly smaller number of vulnerabilities than Linux. Because of its complicated design and enormous code size, Linux is extremely vulnerable to being hacked or attacked by an adversary. The SE2 method is designed to reduce packet transmission delays caused by VM extraction. SE2 may also utilize SR-Lov to separate control panels since packets on each control panel skip the driver domain network stack. The se2 architecture is seen in Figure 1. The solid black and white line represents the data flow, while the dotted line is utilized to configure the network environment. Physical NlC has several virtual maps and a physical role (PF). PF is a physical NlC PCl function that supports SR-Lov capabilities (Lee et al., 2018).

By changing the number of transfers in each VM independently, SE2 may give different functionality between control panels. SE2 can provide a distinct function by allocating more transfers to Substitute A than Substitute B when Substitute A demands more control packages than Substitute B. SE2 allows an index to govern resource allocation based on the purpose and dynamic traffic load from various controller plates.

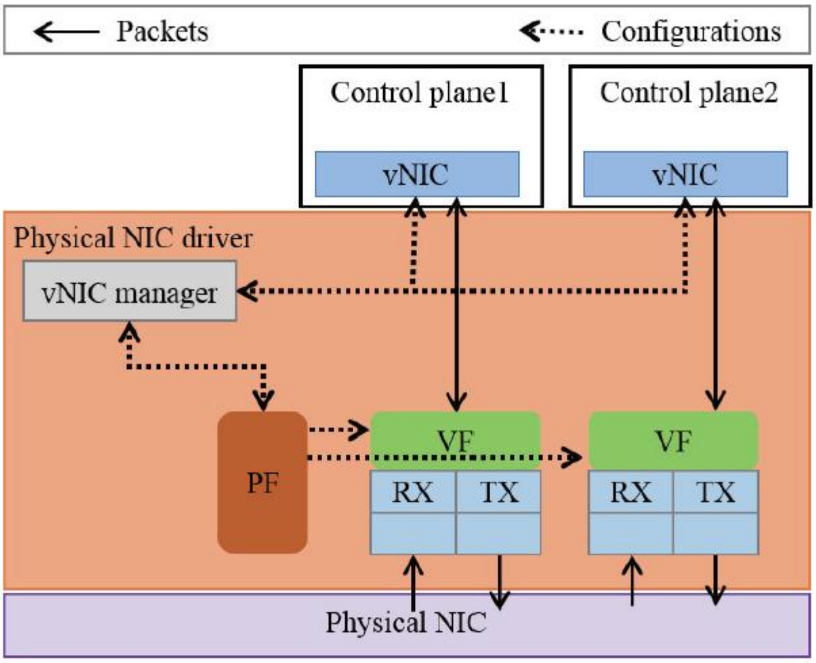


Figure 1. Separate executable environment (SE2) enabled by virtual network graphics card (vNlC), which plays a virtual role (VF) for each page. PF Physical role

3-1-Separate processing of SP2 package

In order to fix the problem, the Linux network stack was bypassed during processing. They substantially enhance packet processing performance by letting user-level programs to directly access intermediate networks. Packets, on the other hand, need the use of many specialized physical cores to handle the input or output. Furthermore, present techniques that circumvent the Linux kernel cause pages to overlap since all processes and boot VMs on a single device share a shared memory repository. Because each control panel in the physical device has access to the primary memory repository, a packet received for a control panel in the memory repository can be utilized on other pages as well. We do not modify the core semantics of Linux, unlike other techniques that go via the Linux network column; instead, we optimize it for improved Linux stack network performance. We created SP2 because it divides complicated packet processing into two phases on Linux, which reduces packet processing time. We enhance the efficiency of controller levels while avoiding control panels from impacting one other by improving the regular processing procedure of Linux packages. The remainder of this section extensively describes and illustrates the Linux network processing procedure in SP2 (Thimmaraju et al., 2018).

The closed processing mechanism in Linux combines Dynamic Memory Access (DMA) activities and CPU performance, as depicted in Figure (2). Linux allocates buffers (RX and TX loops) to storage packages for RX and TX at the start of the installation. The NlC allocated to the descriptors is then declared by writing the address of the descriptors to the registry in (2) NlC, and the DMA of the new descriptors is received (3). The DMA copies the received packet to the memory area connected to the descriptor when a packet enters NlC (4). (5). After the DMA write operation, NlC establishes a hardware interrupt for accepting packets (6). Linux generates a software break using this hardware break, and the accompanying program is known as softirq (Thimmaraju, 2020).

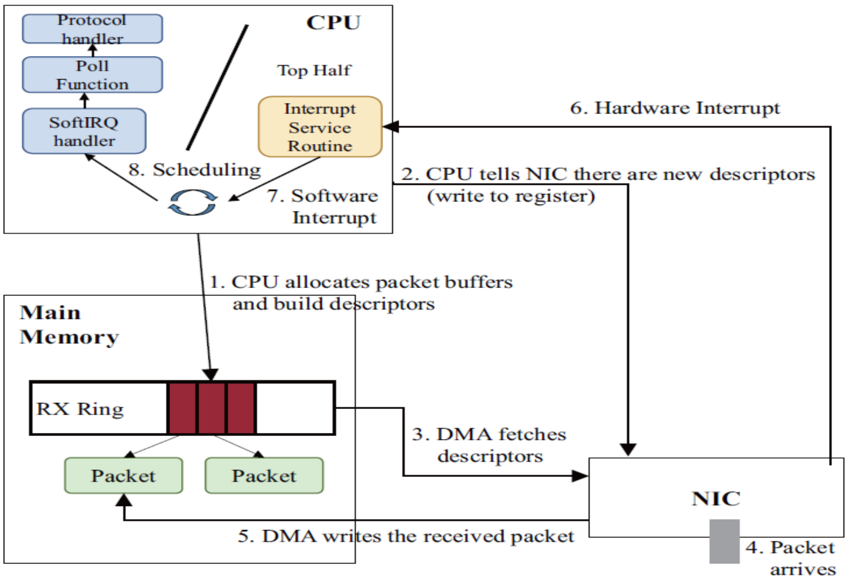

CPU
Top Half
Protocol handler
Poll Function
SoftIRQ handler
Interrupt Service Routine
8. Scheduling
7. Software Interrupt
6. Hardware Interrupt
2. CPU tells NIC there are new descriptors (write to register)
1. CPU allocates packet buffers and build descriptors
Main Memory
RX Ring
Packet
Packet
3. DMA fetches descriptors
NIC
5. DMA writes the received packet
4. Packet arrives

Figure 2. Network processing routine in Linux including Dynamic Memory Access (DMA) and CPU performance

4-1- Implementation

SE2 is a Hyperion 4.0 Xen virtual machine (VM) based on a 2.6.32 Linux kernel image. Early SE2 is used. The NIC ixgbe-3.17.3 virtual driver management network assigns a virtual network device (vNIC) to the VM. Multiple VNICs from separate VMs can program for the same physical NIC at the same time. Each vNIC has its own MAC address, and incoming packets are routed directly to the control panels via the MAC. After the SE2 driver is installed, an alternative can set up a control panel, which includes a controller and a control software, as illustrated in Figure (3). The SP2 benchmark establishes a free lock queue that recovers packets from the reusable buffer after initializing the ixgbevf driver. Furthermore, the SP2 standard creates a central string, known as an SP2 string that processes extra packets such as IP header verification and firewalls. In SP2, we adjust the received performance of the ixgbevf driver to divide the receiving technique based on MPF (PH) and PH) (ixgbevf_clean_rx_irq). The initial half of SP2 is performed by MPF). Only the received packets from a reusable buffer are sent to the unlocked queue in SP2 by the MPF in the ixgbevf drive. Without stopping to process earlier packets, MPF may transfer incoming packets in vNIC to the unlocked center instantly. This speeds up the ixgbevf bootloader's packet processing and allows it to receive more packets. When there are more than one batch of packets in the locked data queue, the SP2 unit acts on the organized data, as shown in Figure (3).

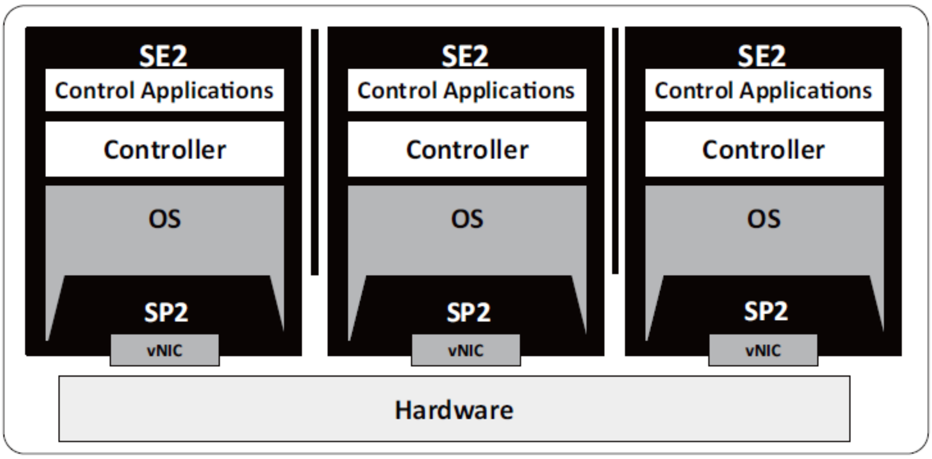


Figure 3. Each control panel contains a separate SE2 and SP2

The performance of the network stack without controllers and SDN control programs is analyzed to view the basic performance of Linux, regardless of the SDN type of controller or control of programs and applications. It employs two physical servers, each with a dual-core dual-core processor, an X8DAH + main board, and 12GB of memory, and is linked to 10GB Internet servers. Three Intel 82599 10Gbps switches with two ports each are used in the SR-IOV. Each control panel's physical NIC interface was given two processors, 2 GB of memory, and two RX / TX queues. Multiple page controls are evaluated to launch up to five times. When the network architecture has 41 edges, three or four controllers are adequate to lower the average network time (Lee et al., 2018). As a result, a maximum of five control levels is enough to support up to 40 servers (Thimmaraju, 2020). Packages ranging from 64 bytes to 1500 bytes are also available. This demonstrates that depending on the network request, monitor control with our SE2 and SP2 can accommodate a variety of control messages (Specification, 2018).

In SE2, VM and SR-IOV were utilized to control the screen from a different executable environment. The performance of SE2 package processing is assessed and compared to Linux. The package size for the evaluation ranges from 64 bytes to 1500 bytes, and the package is processed using a single core. Both Linux and SE2 allow packets in the evaluation. When running SE2 with SP2, it also checks packet processing performance and the IP protocol processor's functionality. As illustrated in the diagram, SE2 only performs half as well as the original at packet acceptance time. SE2 has inferior performance than a non-virtual environment, even with SR-IOV. On packets larger than 1024 bytes, SE2 with SP2 achieves around 80% of SE2 performance, demonstrating that SP2 efficiently decreases packet processing.

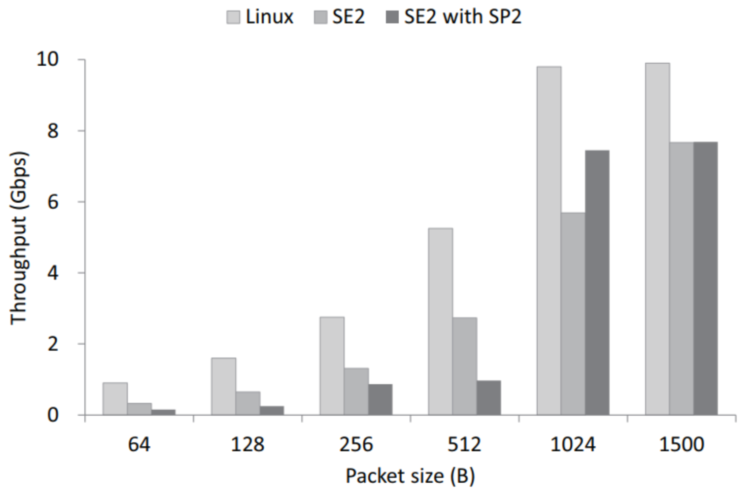
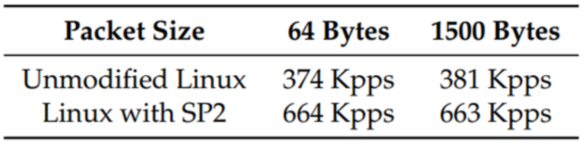


Figure 4. SP2 Minimizes SE2 performance when using VM, which includes 80% native performance in packets larger than 1024

It evaluates how much SP2 improves performance when compared to Linux. When working with IP, the processing speed of Linux and SP2 packages is measured. In this test, inbound traffic is measured with 64 and 1500 byte packets to maximize NIC and CPU processing time, respectively. As seen in Table 1, as compared to Linux, SP2 doubles the packet processing rate. Because Knox SP2 has two distinct cores to control input packets, this is the case.

Table 1. Comparison of packet processing



Packet Size	64 Bytes	1500 Bytes
Unmodified Linux	374 Kpps	381 Kpps
Linux with SP2	664 Kpps	663 Kpps

For 64-byte and 1500-byte packets, SP2 performs up to 74 and 77 percent better, respectively. Furthermore, the screen's control function is monitored in a big reusable buffer. How many packets with the same source / destination are transported from MPF to PH is determined by batch size. The maximum power is attained at eight when the band size is increased from one to 32, as illustrated in Figure 5. This is because copying memory between the reusable buffer and the LFQ takes longer with a larger batch. Even though SP2 uses batching procedures to lower the overhead cost of transferring memory, a bigger batch size does not ensure better packet processing performance.

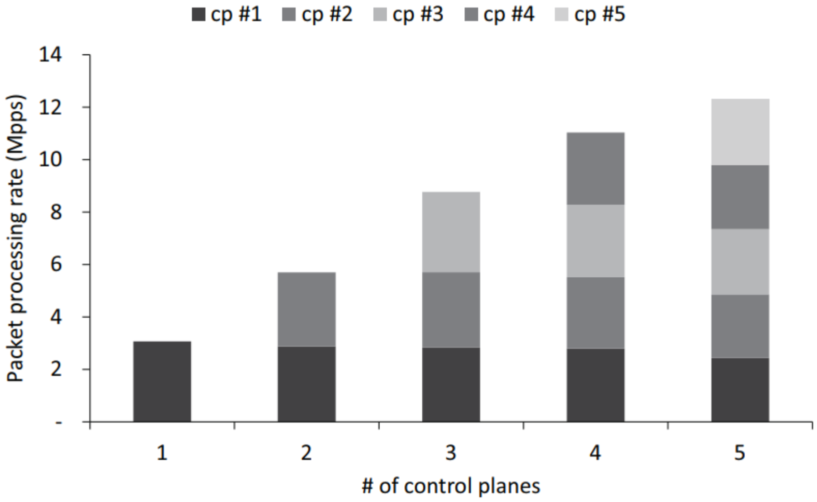


Figure 5. Multifunctional IoT optimization with joint minimization of time and energy

2. Using security framework based on genetic algorithm to improve IoT security

Controlling data access and protecting confidentiality are two critical data outsourcing security considerations. It will be challenging to maintain system performance when several data security risks are considered (CSP, DO and users). DO (Data Owners), CSP (Cloud or Fog Service Provider), and DO-related Many Users are the three entities. Each user is approved in the DO at first (by checking the certificate and other information). Users transmit their relevant certifications and information to the DO during the certification evaluation step. The user certificate is considered to be securely sent to the DO within the registration time. DO transmits the required information (quasi-random number and information relating to counter-jump operations) to the user in a secure response after successful registration. The DO (data owners) is also considered to have certain processing capability and enough storage space to store some data. DO uses CSP to store its data. The user can safely retrieve data from CSP after successful user authentication. It is expected that CSP is aware of and employs data deployment and storage strategies. Such strategies are used by CSPs, which are very huge organizations. The link between DOs (data owners), CSPs (cloud service providers), and users is depicted in Figure (6).

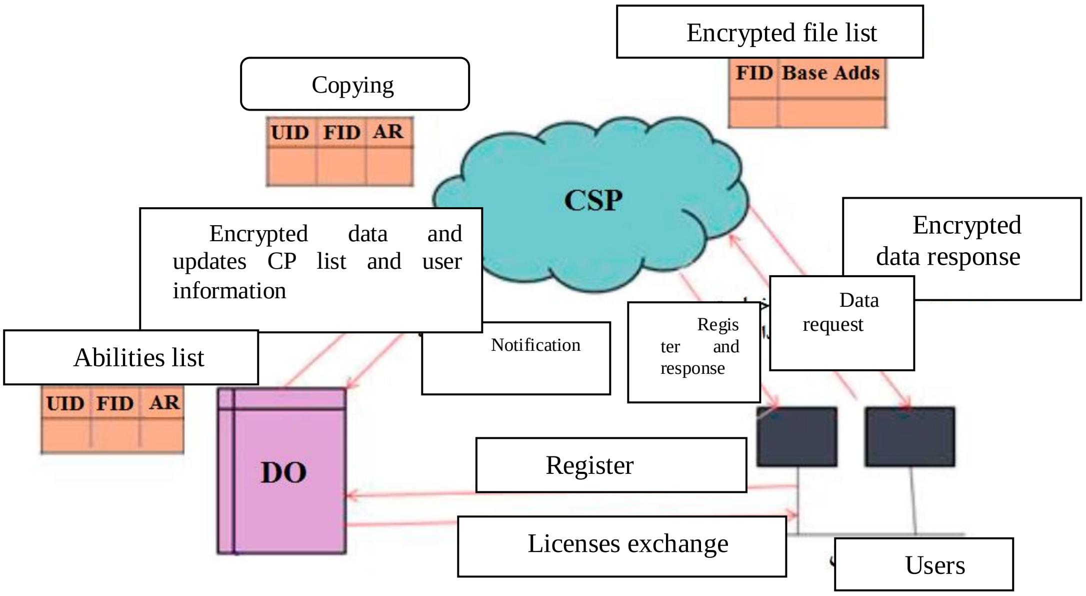


Figure 6. Showing the proposed communication method

A data is converted to ASCII values in this security framework. Following that, the ASCII values are transformed to binary bits. After that, binary bits are separated into blocks of the same size. Block sizes can range from 8 bits to 4 bits to 2 bits and beyond. For the encryption and decryption processes, the Genetic Algorithm (GA) procedures (interaction and mutation) are used. Each pair of blocks is subjected to GA procedures. Each GA operation's final output is encrypted text, which is also a pair of blocks of bits. Each encrypted text in the cloud is kept in a separate location, and the position of the encrypted text is not fixed with some approaches (for example, output 1 in the cloud, which is at l 1 at time t 1, could be at time t 2). Make sure you're in the right spot l 2). CSP is unable to see encrypted data since portions of it are stored in the cloud. These bits of data are encrypted with the Data Owners' Private Key (DO) to authenticate the data owners before being transferred to CSP, and then the encrypted data is encrypted with the CSP public key to prevent the attacker from seeing the data or the CP list. Figure (7) depicts the entire operation in 2019).

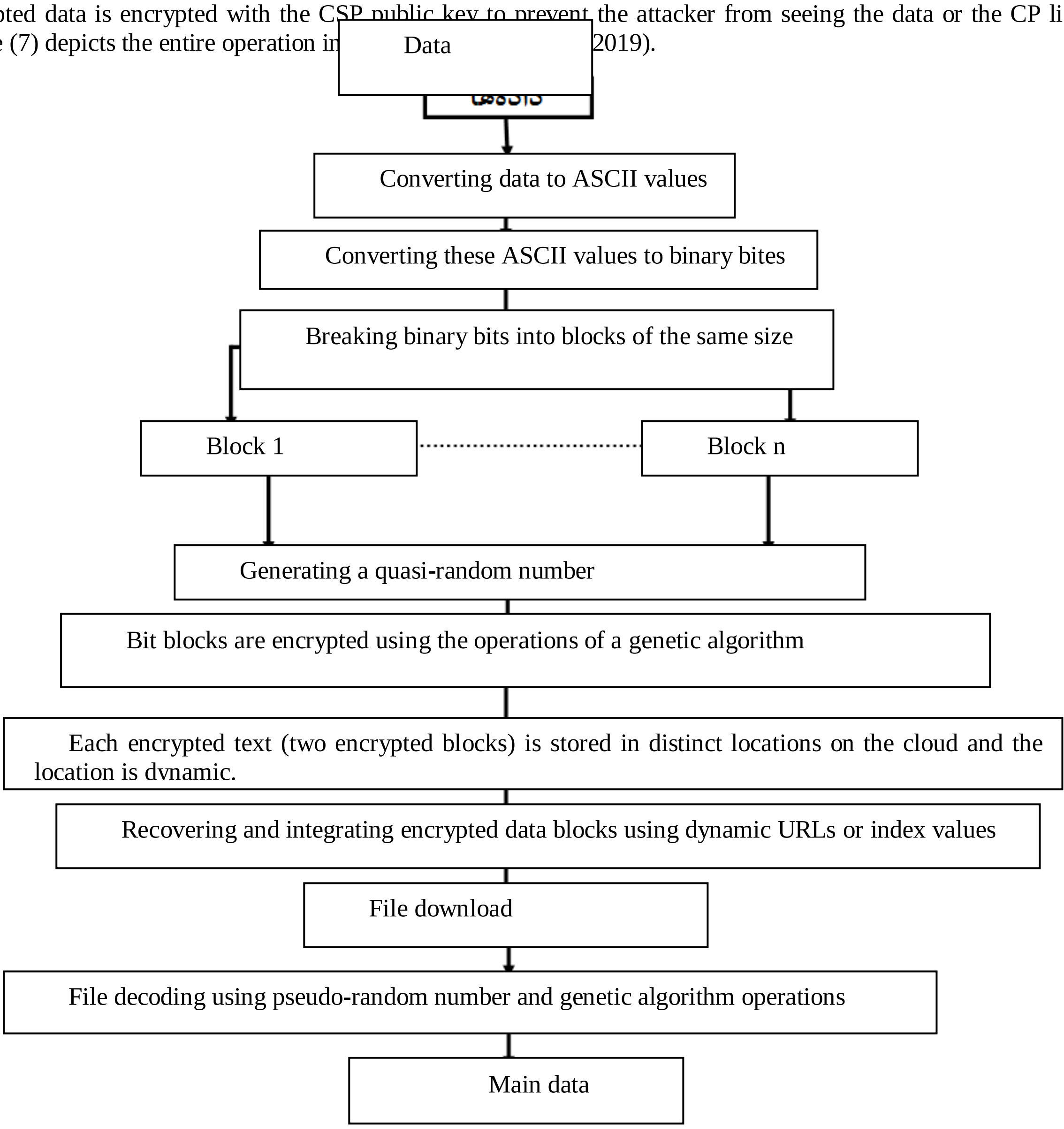

Data
Converting data to ASCII values
Converting these ASCII values to binary bites
Breaking binary bits into blocks of the same size
Block 1
Block n
Generating a quasi-random number
Bit blocks are encrypted using the operations of a genetic algorithm
Each encrypted text (two encrypted blocks) is stored in distinct locations on the cloud and the location is dvnamic.
Recovering and integrating encrypted data blocks using dynamic URLs or index values
File download
File decoding using pseudo-random number and genetic algorithm operations
Main data

Figure 7. Security framework using genetic algorithm

3. LPWAN technology

More than 50 billion devices will be connected to the internet via radio by 2020. Low power networks (LPWANs) have become a popular low-rate broadband radio communication technology because to the rapid growth of the Internet of Things (IoT) sector. The three top LPWAN technologies that compete with large-scale IoT are Sigfox, LoRa, and NB-IoT. Short-range radio technologies (such as ZigBee and Bluetooth), which are commonly utilized, are not ideal for applications requiring broadband transmission. More coverage is possible with cellular communication systems and approaches (such as 2G, 3G, and 4G), but they consume more energy.

As a result of the demands of IoT applications, new wireless communication technologies such as low-power broadband have emerged (LPWAN). As demonstrated in Figure, LPWAN is ideal for IoT applications since it only requires the transfer of relatively tiny amounts of data over a long distance (8). The term LPWAN did not exist until early 2013. In the allowed and illegitimate frequency bandwidth, many LPWAN solutions have arisen. Sigfox, LoRa, and NB-IoT are three of the most recent pioneering technologies, each with its own set of technological distinctions (Albugmi et al., 2016).

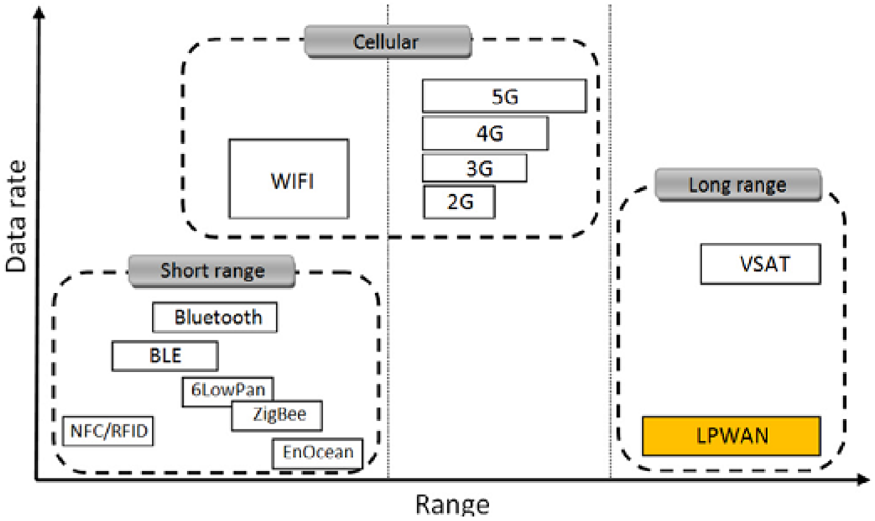


Figure 8. Rates of data required versus domain capacity of radio communication technologies: LPWAN positioning

Table 2. An overview of LPWAN technologies: Sigfox, LoRa, NB-IoT

	Sigfox	LoRaWAN	NB-IoT
modulation	BPSK	CSS	QPSK
Frequency	Unauthorized ISM band (868 MHz in Europe, 915 MHz in North America and 433 MHz in Asia)	Unauthorized ISM band (868 MHz in Europe, 915 MHz in North America and 433 MHz in Asia)	LTE frequency band allowed
Bandwidth	100 Hz	250 and 125 kHz	200 kHz
Maximum data rate	100bps	50kbps	200kbps
Bilateral	Limited / semi-duplex	Yes / semi-duplex	Yes / semi-duplex
Maximum message / day	140 (UL), 4 (DL)	Unlimited	Unlimited
Maximum useful load length	12 bytes (UL), 8 bytes (DL)	243 bytes	1600 bytes
Interference safety	Very high	Very high	loq
Authentication and encryption	Not supported	Yes (AES 128b)	Yes (LTE encryption)
Compatible data rates	No	No	No

Delivery	The end device is not connected to the base station	The end device is not connected to the base station	The end device is connected to the base station
Location	Yes (RSSI)	Yes (TDOA)	No (under review)
Standardization	Sigfox is partnering with ETSI on Sigfox-based network standardization	LoRa-Alliance	3GPP

When selecting the correct LPWAN technology for IoT applications, many criteria must be examined, including service quality, battery life, latency, scalability, payload length, coverage, range, expansion, and cost. Sigfox, LoRa, and NB-IoT are contrasted in terms of these criteria as well as their technical differences in the table below.

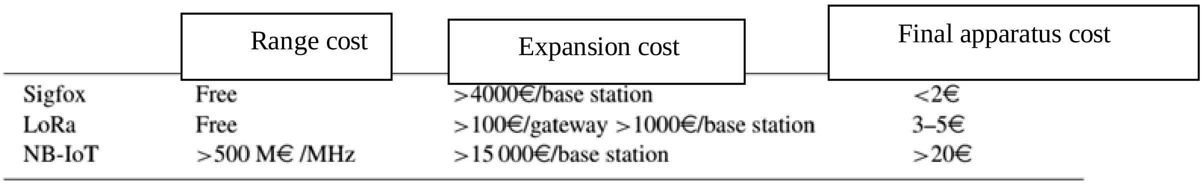
Services quality

Unauthorized spectrum and asynchronous communication techniques are used by Sigfox and LoRa. They are unable to employ the same quality of service provided by NB-IoT. The auction of allowed LTE bandwidth is over € 500 million per MHz, because NB-IoT uses authorized bandwidth and LTE-based synchronization algorithms, which are cost-effective for QoS. NB-IoT is suitable for applications that require quality assurance of services due to cost and QoS exchange, whereas applications that do not have this limitation should use Sigfox or LoRa (Reynders et al., 2016).

Battery life and latency

The majority of the time, the final devices in Sigfox, LoRa, and NB-IoT are in sleep and non-operation mode, which decreases the amount of energy consumed and so extends the life of the devices. Due to synchronization and QoS, the ultimate NB-IoT device requires more power, and OFDM / FDMA access modes demand more peak current. In comparison to Sigfox and LoRa, the higher power consumption affects the life of the final NB-IoT device. NB-IoT, on the other hand, has a low latency advantage. Unlike Sigfox, LoRa provides Class C to take advantage of reduced two-way latency while consuming more power. As a result, Sigfox and Class A LoRa are the best solutions for applications that aren't sensitive to latency and don't send a lot of data. NB-IoT and LoRa Class C are the best solutions for applications that demand low latency.

Table 3. Different costs of Sigfox, LoRa, NB-IoT



	Range cost	Expansion cost	Final apparatus cost
Sigfox	Free	>4000€/base station	<2€
LoRa	Free	>100€/gateway >1000€/base station	3–5€
NB-IoT	>500 M€ /MHz	>15 000€/base station	>20€

Scalability and useful load length

One of the important advantages of Sigfox, LoRa, and NB-IoT is their support for a large number of devices. These technologies improve as the quantity and volume of linked devices grows. To deal with this scalability aspect, several strategies are being examined, including effective channel diversity, time, and space utilization. NB-IoT, on the other hand, has a significant scaling advantage over Sigfox and LoRa. NB-IoT allows almost 100K terminal devices to be connected per cell, compared to 50K for Sigfox and LoRa. The NB-IoT, on the other hand, has the benefit of a maximum useful load length. As seen in Table (3), NB-IoT enables for roughly 1600 bytes of data transfer. LoRa enables for the transmission of up to 243 bytes of data. Sigfox, on the other hand, has a minimum practical load length of 12 bytes, which limits its applicability in IoT applications that demand huge amounts of data.

Network coverage and domain

The fundamental advantage of Sigfox is that a single base station can cover a whole city (range > 40 km). With only seven base stations, the Sigfox network covers the entire country of Belgium, which covers an area of around 30,500 km2 (Sinha et al., 2017). LoRa, on the other hand, has a modest slope (range 20 km) and only three base stations are needed to cover a whole metropolis, such as Barcelona. NB-IoT has the shortest range and coverage (around 10 kilometers). NB-IoT is mostly based on devices that are put in cellular network's remote areas (e.g., internal, external). Furthermore, the spread of NB-IoT is confined to LTE base stations. As a result, it is not ideal for rural or suburban locations where LTE service is not available.

Expansion model

NB-IoT specifications released in June 2016; therefore, it will take more time before it can be networked. However, the Sigfox and LoRa ecosystems are mature and are now commercialized in many countries and cities. Compared to Sigfox, which is used in 31 countries, LoRa has the benefit of being used in 42 nations. However, Sigfox's LoRa network continues to grow around the world. Furthermore, the LoRa ecosystem's adaptability is a significant benefit. Unlike Sigfox and NB-IoT, LoRa promotes the extension of local area networks, or LANs, as well as the deployment of public networks via base stations. The hybrid start-up approach can be utilized in the industrial setting to extend the local LoRa network in production areas and the public LoRa network to reach external areas (Sinha et al., 2017).

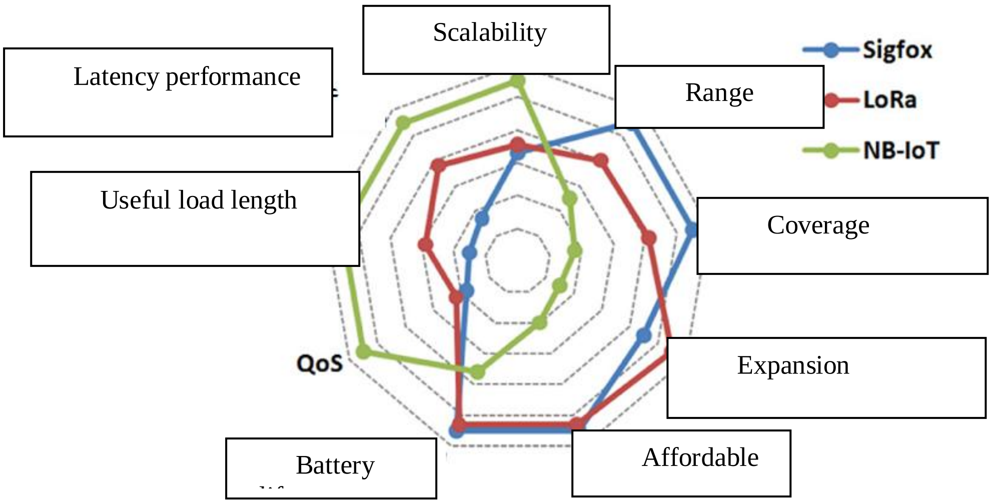


Figure 9. Advantages of Sigfox, LoRa, NB-IoT in terms of IoT factors

Cost

Various cost factors need be addressed, including spectrum (licensing) costs, network / development costs, and device costs. The costs of Sigfox, LoRa, and NB-IoT are shown in Table (4). Sigfox and LoRa have shown to be more cost-effective than NB-IoT. In conclusion, Sigfox, LoRa, and NB-IoT each have their own advantages in terms of various IoT elements, as shown in Figure (10). The Sigfox LoRa device will be low-cost, have a large range (high coverage), a low connection rate, and a long battery life. Unlike Sigfox, LoRa will use a local area network to enable reliable connectivity for devices traveling at fast speeds. NB-IoT, on the other hand, will cater to high-value IoT industries prepared to pay for low latency and high-quality services.

In addition to cellular testing, the NB-lack IoT's of commercial development raises concerns regarding the technology's actual battery life and performance in the real world. Finally, by 2020, 5th generation (5G) wireless mobile communication is predicted to enable global human and device connection, paving the way for a global LPWAN solution for IoT applications.

4. Using blockchain in the Internet of Things

Blockchain, a distributed technology, was designed with cryptocurrencies like Bitcoin in mind. Satoshi Nakamoto developed the concept of the Chinese blockchain in 2008, and it has gained a lot of interest in recent years as an emergent peer-to-peer (P2P) computing and decentralized data sharing technology. Blockchain can avoid attacks on the control system by utilizing cryptographic technology without the usage of centralized actor control or centralized data storage. Later, in 2013, Ethereum was released as a transaction-based machine mode for planning and programming blockchain technology. Blockchain has been employed in various fields beyond cryptocurrencies because of its unique and appealing qualities such as transaction confidentiality, security, data non-imitation, audibility, integrity, authentication, system transparency, and fault tolerance.

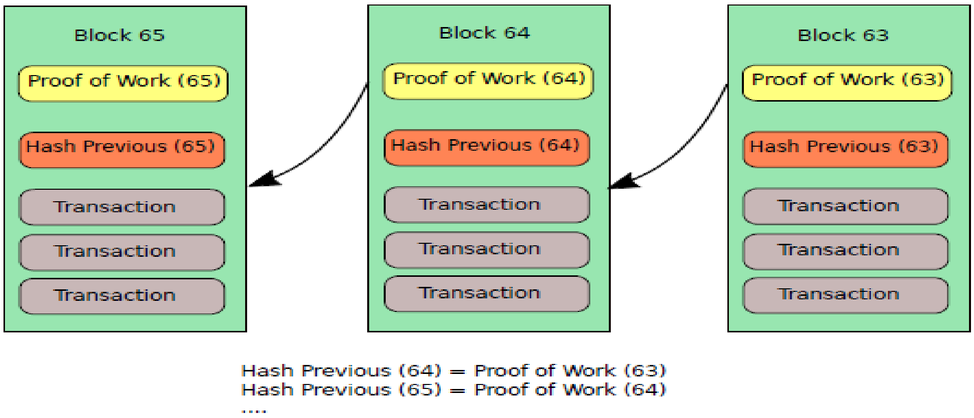


Figure 10. Blockchain structure

He proposed a distributed access control system based on blockchain technology to govern IoT items. This system's design is made up of six parts: 1) wireless sensor networks, 2) wireless sensor networks, and 3) wireless sensor networks. 2) supervisors, and 3) broker nodes 4) Contracts with smart features 6) hubs or management centers for blockchain networks. The system has several advantages for IoT access control, including 1) mobility, which can be utilized in isolated management systems, 2) accessibility, which ensures that access control rules are always available, and 3) concurrency, which allows access control policies to be amended at the same time. 4) The system is light weight, which implies that IoT devices must be changed to work with it. 5) Scalability, because IoT devices can be connected via a variety of constrained networks; 6) Transparency, so the system can protect a location's privacy.

Blockchains can improve the Internet by allowing users to subscribe to trusted subscription services that can be tracked and verified. Data sources can be identified at any time, and the data stays the same throughout time, increasing its security. This integration is a game-changer in situations when IoT data needs to be securely shared among a large number of people. A vital part of guaranteeing food safety, for example, is detailed tracking of various food products. Many people are involved in food tracking, including those involved in production, nutrition, treatment, distribution, and so on. Data leaks at any point in the chain can lead to fraud and slowed infection detection, which can have a significant impact on citizens' lives and cost enterprises, departments, and agencies a lot of money. Better control in these regions boosts food security, enhances data sharing among participants, and shortens the time it takes to find disease outbreaks, potentially saving lives.

Conclusion

Many of the items and equipment around us that are connected to the Internet and can be controlled and managed by programs on smartphones and tablets are referred to as the Internet of Things. The Internet of Things is based on wireless radio waves that allow various devices to connect with one another over the Internet, or, in other words, the concept of building various objects with the ability to communicate wirelessly for interception and control through the Internet. Even a simple smartphone app can define the term Internet of Things. The ideal IoT would use little energy, be intelligently programmed, and be able to receive data fast and correctly over a long length of time. It would also be easy to set up and maintain. One of the key aspects of this grid is the two-way smart grid, which allows users to report the quantity of energy produced and used to the grid. Within a country, this relationship can be defined. Wireless networks that send information in two directions can be monitored, repaired, and maintained in real time. Hundreds to thousands of nodes can be found in a network, each of which can record and communicate physical or environmental changes. As a result, it's used in a variety of projects, such as wind and solar generating plants. Because all items use the Internet to exchange data, the Internet of Things has raised a number of security challenges and worries about end-user privacy. Even with all of its advanced information exchange capabilities, the Internet of Things is a security vulnerability, and it must take proper actions in its early stages to ensure widespread and successful adoption before going on to the next level of growth.

References

Safari, Muslim. (2015). IoT security and privacy concerns. The first national conference on computer, information technology and Islamic communications in Iran.

Albugmi, A., Alassafi, M. O., Walters, R., & Wills, G. (2016). Data security in cloud computing. 2016 Fifth international conference on future generation communication technologies (FGCT).

Hakiri, A., Sellami, B., Patil, P., Berthou, P., & Gokhale, A. (2017). Managing wireless fog networks using software-defined networking. 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA).

Lee, K., Lee, C., Hong, C.-H., & Yoo, C. (2018). Enhancing the isolation and performance of control planes for fog computing. *Sensors*, *18*(10), 3267.

Liu, Y., Xiong, K., Zhang, Y., Zhou, L., Lin, F., & Liu, T. (2019). Multi-objective optimization of fog computing assisted wireless powered networks: Joint energy and time minimization. *Electronics*, *8*(2), 137.

Moreno-Vozmediano, R., Montero, R. S., Huedo, E., & Llorente, I. M. (2017). Cross-site virtual network in cloud and fog computing. *IEEE Cloud Computing*, *4*(2), 46-53.

Reynders, B., Meert, W., & Pollin, S. (2016). Range and coexistence analysis of long range unlicensed communication. 2016 23rd International Conference on Telecommunications (ICT).

Sen, J. (2013). Security and privacy challenges in cognitive wireless sensor networks. In *Cognitive radio technology applications for wireless and mobile Ad hoc networks* (pp. 194-232). IGI Global.

Specification, O. S. (2018). Retrieved August 16 from https://www.opennetworking.org/wp-content/uploads/612014/10/openflow-switch-v1.5.1.pdf.

Thimmaraju, K. (2020). From threats to solutions in data center networks.

Thimmaraju, K., Shastry, B., Fiebig, T., Hetzelt, F., Seifert, J.-P., Feldmann, A., & Schmid, S. (2018). Taking control of sdn-based cloud systems via the data plane. Proceedings of the Symposium on SDN Research.

Yi, S., Li, C., & Li, Q. (2015). A survey of fog computing: concepts, applications and issues. Proceedings of the 2015 workshop on mobile big data.

Yu, J., & Buyya, R. (2005). A taxonomy of workflow management systems for grid computing. *Journal of grid computing*, *3*(3-4), 171-200.