Jordanian Journal of Computers and Information Technology (JJCIT), Vol. 06, No. 04, December 2020.

CLOUD OF THINGS: ARCHITECTURE, RESEARCH CHALLENGES, SECURITY THREATS, MECHANISMS AND OPEN CHALLENGES

Shamsul Haq, Adil Bashir and Sahil Sholla

(Received: 13-Jun.-2020, Revised: 9-Aug.-2020 and 6-Sep.-2020, Accepted: 9-Sep.-2020)

ABSTRACT

In this era of communication and networking technology, Internet of Things adds to the existing technological era and brings revolution to the Information Technology world. Internet of Things consists of interconnected devices which may be digital, physical or mechanical devices equipped with unique identifiers and having the capability to transmit the sensed information to other devices autonomously. Internet of Things is recognized as being composed of resource constraint devices in terms of processing competency, storage capacity and power resources. To cope up these constraints, existing computing technology known as cloud computing can be used to facilitate the Internet of Things system by offloading its processing and storage requirements. In this paper, we have provided the necessity and benefits of Cloud and IoT integration. Further, the paper has identified several research issues that arise due to Cloud-IoT integration. Among the several research issues, it was observed that security and privacy concerns are pivotal in Cloud-IoT integration and need to be addressed to make the integration successful. The core security and privacy threats have been identified and the existing security mechanisms have also been researched in this paper. The paper also highlights open security and privacy research issues in the Cloud-IoT paradigm. This paper can act as a baseline for the research that is needed in the area of security and privacy issues in the Cloud-IoT or Cloud of Things paradigm.

KEYWORDS

Internet of things, Cloud computing, Cloud of things, Security, Privacy, Encryption algorithms.

1. INTRODUCTION

Internet of Things (IoT) is a networking paradigm that connects billions of heterogeneous devices, called Things, within the same backbone, essentially, the Internet. These connected things sometimes referred to as objects, have the ability to generally capture environmental data using dedicated sensors, process the acquired data and communicate the data with other things, within the framework of a smart application [1]. According to the definition of Internet Architecture Board (IAB), IoT is a network of smart things and a way of intelligent communication among an enormous number of connected devices that use a new version of internet protocol (IPV6) providing 2^{128} unique addresses, capable of realizing the actual concept Internet of Things. IoT is swiftly growing and is expected to connect billions of objects in the near future, which requires billions of network addresses. The IoT in whole can be said as an innovation to put together smart things, frameworks and sensors [2]-[4]. The basic building blocks of IoT include hardware, embedded programming and wireless communication technologies. The core of any IoT infrastructure is billions of interconnected devices containing sensors and actuators to sense or detect any physiological or environmental phenomenon. Notwithstanding, to transmit the information that the devices gather, these devices require handling and processing abilities, so that the data can be structured and formatted for transmission. This handling and processing function is commonly performed by a micro-scale integrated circuit; for example, a System-on-a-Chip (SoC) or a Field-Programmable Gate Array (FPGA). Since IoT devices are embedded devices, they are prototyped using competitive micro-scale platforms; for example, Arduino, Phidgets and Raspberry Pi. Prototyping IoT devices using these platforms requires micro-scale controller programming, circuit construction abilities and profound knowledge of hardware communication standards, such as I2C or SPI, that are used to build communication between the micro-scale controller and the associated sensors and actuators. The embedded programs are regularly developed using computer programming languages such as C, C++, Python and JavaScript.

S. Haq, A. Bashir and S. Sholla are with Department of Computer Science and Engineering, IUST, Awantipora, J&K, India. Emails: s.haq266@gmail.com, adilbashir.445@gmail.com and sahilsholla@gmail.com

IoT is becoming an important and globally used technology because of its remote sensing, monitoring and controlling of object (physical and virtual) services across the existing network-infrastructure to enable direct physical world integration with the computer-based systems. It improves the efficiency and accuracy of objects reduces the intervention of humans and provides safety and convenience. To organizations, the benefits offered by IoT include monitoring of the overall business process, improving the experience of customers, saving money and time and making better product decisions. Generally, it is becoming more abundant and important in transportation, manufacturing and utility organizations, as well as in agriculture, home automation, smart cities and smart healthcare [5]-[6]. The layered architecture of IoT consists of five layers; i.e., Perception Layer, Transport Layer, Processing Layer, Application Layer and Business Layer, as shown in Figure 1 [2]-[3].

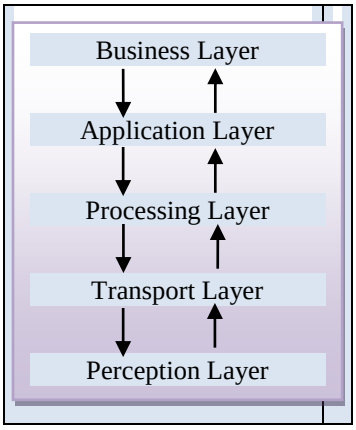

Figure 1. IoT architecture [2]-[3].

1.1 Perception Layer

It is also known as the sensor layer. Its responsibility is to sense the environmental or physiological data of the environment in which it is implemented. The devices are identified and tracked using identification mechanisms, such as RFID tags. Further, the sensor measurements are detected and transformed into electric signals.

1.2 Transport Layer

The services provided by the transport layer include the transmission of information to the processing layer as well as confirming that the information is from the valid user and protecting it from threats using different security protocols. An authentication mechanism based on pre-shared secret keys or passwords is used to verify the valid user.

1.3 Processing Layer

The transport layer sends the information to the processing layer in order to process the collected information. The processing layer removes any extra insignificant information and extracts useful information from the data sent by the transport layer.

1.4 Application Layer

All applications that are using the technology of IoT are defined in the application layer, such as smart cities, smart homes, …etc. The core responsibility of this layer is to provide services to the applications. For each type of application, there may be varying services because of dependent on information collected by sensors.

1.5 Business Layer

It intends the behaviour of an application and is acting as a manager of the whole system. Its responsibility is application control management, business and profit models in IoT. The privacy of users is also managed by this layer [7]-[11]. IoT finds its applications in almost every field, such as industrial automation, supply chain management, intelligent transportation, smart cities and smart

healthcare. However, the IoT devices are characterized by constrained resources that hinder their application in sensitive areas where the information needs to be kept secure and safe.

Another important technology, known as cloud computing, enables the development of ubiquitous computing *via* on-demand and convenient access to a configurable shared pool of computing resources, such as network servers, applications, storage and services that can be distributed and released rapidly with less effort and interaction by service providers. Cloud computing is generally divided into two segments; namely, front-end and back-end, based on the architectural viewpoint, as shown in Figure 2 [12].

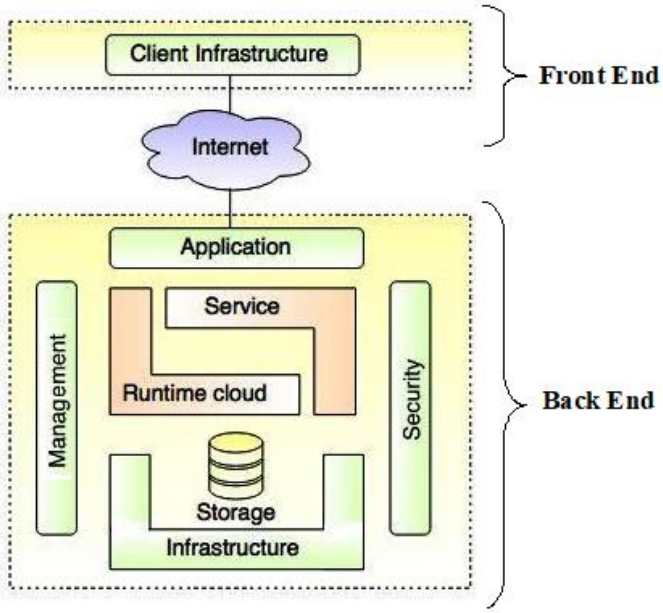

Figure 2. Cloud architecture [12].

The two segments are connected to each other through a network, usually *via* the Internet. The services provided by cloud to its users include Software as a service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) [12]-[13]. The benefits provided by the cloud include improvement in performance, massive data handling, minimum issues of maintenance, recovery and backups and scalability [14]-[16].

The greater enhancements in the fields of wireless sensor networks, ubiquitous computing and machine-to-machine (M2M) communication make IoT a more popular and preferred technology. However, IoT devices are resource-constrained, location-specific and inflexible. On the other hand, cloud computing resources are ordinarily area-free (location-independent) and inexpensive, while simultaneously providing fast and precise elasticity. Therefore, to alleviate incompetence in IoT, the Cloud can play a significant role, which necessitates the integration of IoT with the Cloud.

Cloud-IoT is an emerging concept, where the limitations put forth by IoT devices are somewhat addressed using cloud computing services. There are various architectures proposed for Cloud-IoT and most of them focus on data sharing, monitoring, …etc. while using services of the cloud. Though the architectures are varied, some parts among them are common. The simple architecture of Cloud-IoT is shown in Figure 3. The most common elements in Cloud-IoT architectures are:

a) Sensors: Sensors are used to gather data from the deployed environment or objects, such as animals, people, devices, buildings, cities, …etc. The information gathered can be categorized based on sensor type (heterogeneous or homogeneous), sensor methodology (passive or active) or sensing parameters (like body temperature, ECG system, …etc.). The collected data is made available on the cloud [17]-[19].

b) Cloud software: It is responsible for storing and processing information obtained from IoT devices and environments [17]-[19]. It also provides different services for the IoT components, such as monitoring, hosting and managing devices.

c) Network components: These refer to the equipment used for data transmission. Gateways or device

drivers are commonly used equipment for the communication between the software components and devices [17]-[18], [21].

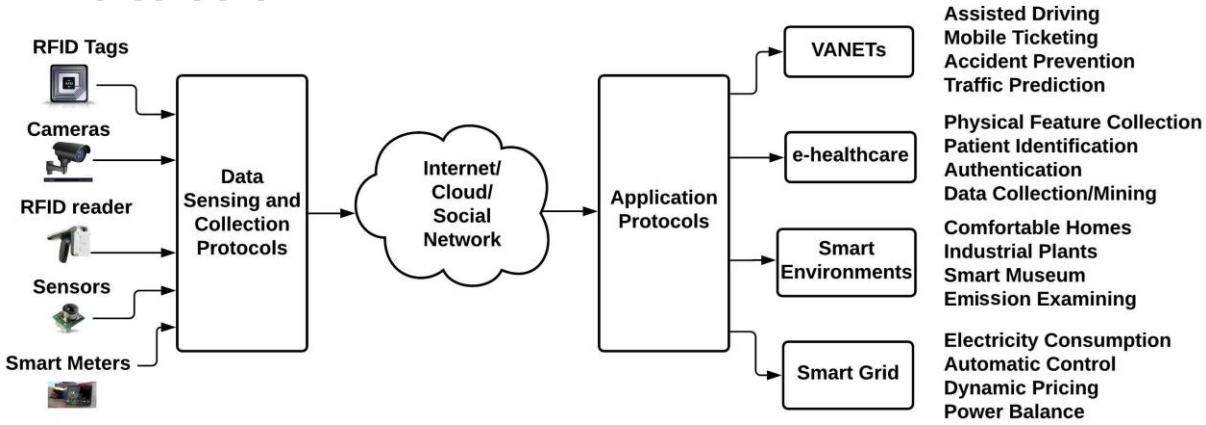

Figure 3. Cloud-based IoT architecture [17].

The rest of the paper is organized in the following sections. Section 2 discusses the importance and benefits of Cloud and IoT integration. Section 3 further explains the research issues in Cloud-IoT integration. Section 4 discusses the security aspects of Cloud-IoT integration. The state-of-the-art security mechanism in Cloud-IoT infrastructure is presented in Section 5 and in Section 6, the open challenges and issues in Cloud-IoT are presented. Section 7 concludes the paper.

2. IoT AND CLOUD INTEGRATION

The current insurgency in the world of information and communication technology (ICT) is equipped by the IoT and services of cloud computing. This offers more open doors for the development of new systems whose main aim is to facilitate the lives of individuals and take out the conventional complexities confronting them. The proliferation of cloud computing and IoT technologies will facilitate new controlling services by handling and processing large volumes of sensory-data streams. Cloud computing is expected to support a wide scope of IoT applications; for example, smart homes, smart cities, smart e-health services, smart buildings, smart grids and so forth [20]. The cloud and IoT are different technologies having different evolutions. The comparisons of cloud and IoT are shown in Table 1. They have complementary characteristics due to which a number of researchers are motivated to test the integration of these two technologies [13]-[14]. The unlimited resource capabilities in terms of processing, communication and storage capacity of the cloud can benefit the IoT and in return, the cloud can get benefited from IoT's rapidly developing services and getting the opportunity to interact with real-world objects [17]-[18]. Some of the main features and characteristics which relate to both Cloud and IoT include services over the internet, storage over the internet, applications over the internet, energy efficiency and computational capability. The features offered by IoT and Cloud computing are shown in Table 2. Table 2 aims at explaining the enumerated characteristics of cloud technologies that are closely linked to IoT. The observations from Table 2 reveal that IoT characteristics that are more influenced by cloud characteristics are sensors in households and at airports. Concerning cloud computing, the most affected characteristics are services over the internet

Table 1. Comparison of cloud computing with IoT [17].

ITEMS	CLOUD COMPUTING	IoT
Big Data	To manage the enormous big data	Source of big data
Storage capabilities	Unlimited capabilities of storage	Limited or no capabilities of storage
Connectivity	Use of internet for services to deliver	Use of internet for the point of convergence
Processing capabilities	Virtually unlimited capability of computation	Limited capabilities of computation
Characteristics	Ubiquitous (availability of resources from everywhere) The resources are virtual	Pervasive (things are at everywhere) The objects are of real world

and computational capacity. The overall inference that can be drawn is that these two technologies contribute more to each other in many of their characteristics.

Table 2. Contributions of cloud computing and internet of things [18].

IoT Characteristics	Storage over Internet	Service over Internet	Applications over Internet	Energy Efficiency	Computational Capability
Smart Grids	X	X	-	X	X
Intelligent Transportation	X	X	X	-	X
Sensors installed at homes and airports	X	X	X	X	X
Smart Healthcare	-	X	X	-	X
Engine monitoring sensors	-	X	X	X	X

2.1 Integration Benefits of IoT and Cloud Technologies

IoT is bringing revolution to all the application areas and has made a homogeneous impact on the technology. However, the integration of IoT with cloud put forth several advantages, some of which are presented below [21]-[28].

2.1.1 Scalability

One of the biggest advantages of Cloud-IoT integration is scalability. In case of complex infrastructure of networks, scaling up needs purchasing extra hardware, investigating extra time and undertaking greater configuration and design efforts become difficult. In Cloud-IoT systems, also known as Cloud of Thing (CoT), adding new resources mainly boils down to leasing other virtual servers or extra cloud space which provides the extra benefit of being rapidly implemented. Moreover, the services of the Cloud-IoT platform offer flexibility, providing storage as per requirements and scaling down the number of IoT-enabled systems.

2.1.2 Cost-effectiveness

Large starting upfront investments and expanded implementation risks in the occurrence of in-house IoT systems can be debilitating. Added to that, there is a high concern for the continuous expenses of hardware maintenance (upkeep) and IT personnel (faculty). Fundamentally, scaled-down direct expenses and an adaptable valuing scheme dependent on real utilization urge IoT-based enterprises to change to the cloud. Inside this business model, costs are simpler to anticipate and fewer costs to incur about the hardware equipment failures, which in case of in-house IoT systems may create extra expenses, not to cite business misfortunes resulting from service halts and downtimes.

2.1.3 Improved Processing Capabilities

The limited processing capacity present in IoT nodes and the enormous volumes of data generated by these miniature nodes can be stored, processed and analyzed in the cloud. To find out the solutions, the cloud provides unlimited virtual capabilities of processing and on-demand services or model of usage. There are decision-making and predictive algorithms that can be integrated with the IoT to reduce risks and increase the revenue at a lower cost [26]. Further, the pathways for transfer, storage and maintenance of data are being created by the cloud.

2.1.4 Remote Access (Geographic Bound)

As the growth of the internet is rapid, IoT systems are growing rapidly and are the next step in the near future. This way, various tasks, like monitoring, performance check, data collection and software up-gradations, can be time-consuming and costly processes. However, cloud computing in IoT assists in the immediate accessing and storing of data remotely. This is an essential trait and is not bound geographically and therefore can allocate recourses quickly at different areas. Due to this advantage, there are greater benefits such as that some of the applications can report their status, process the data remotely and send remote messages to inform their administrator about some of the incidents, …etc. [27]-[30].

2.1.5 Data Integration

With the presentation of IoT in business models, organizations are battling with information support. The issue is not just because a lot of information is generated from a wide range of gadgets and devices, but the variety of information that is being generated by smart IoT devices. Furthermore, there is pre-existing traditional information held in these organizations that is being transferred to servers through internet resources. The management of diverse information types is a daunting task for IT designers and executives, because such information is a significant resource of an organization. Cloud computing can help in managing such diverse information from sensors and already held information of organizations by providing a framework with practically no constraints that can scarcely ever be imperilled, because the information is maintained at various separate servers. Along these lines, even in instances of abrupt catastrophes, the cloud will retain the information. Along with these benefits, companies are continuously increasing solutions of clouds as trusted and preferred approaches.

3. RESEARCH ISSUES IN CLOUD-IOT

The transfer of data from the real world to the cloud is made possible by the integration of the cloud with IoT. However, there are various challenges to achieve integration benefits, such as heterogeneity, platforms, services and operating systems, which are particular for the development of new applications. The heterogeneity exacerbates when the approaches of multi-cloud are adopted by the end-users and thus, improving the resilience and performance of applications to services will depend on multi-providers [6]. The big data generated from the expected 50 billion IoT devices in the near future requires having more awareness for its secure communication, access, storage and processing. The important issues that need to be addressed include:

3.1 Interoperability

Interoperability is defined as the ability, due to which heterogeneous devices and platforms can coordinate with each other successfully. It is vital for the interconnection of multiple things together among different networks of communication. If we consider an example of devices in a home automation system that consists of fire detectors, surveillance camera, smoking alarms, entertainment systems, lighting systems, …etc., various protocols are needed for these devices to work in tandem. However, to achieve interoperability, there are various types of challenges to be encountered and dealt with. Some of them are presented below.

3.1.1 Proprietary Ecosystem

It is one of the challenges in interoperability, as proprietary protocols are made by some manufacturers, thus preventing other companies from utilizing them, which makes it difficult to have interoperability.

3.1.2 Cost Constraint

It is another challenge in ensuring interoperable services that are generally faced while designing the gateway solutions. There are certain issues while designing newer protocols, such as the existence of legacy protocols that make it slightly difficult for IoT to use newly designed protocols. Additionally, the technical risks of new protocols may have a higher failure rate.

3.1.3 Scalability

IoT is entering all fields of application, such as transportation, smart buildings, supply chain management, …etc. and the number of devices is increasing rapidly. Therefore, manufacturers are keen to think there would not be an issue of scalability, if for a large number of devices, newer protocols are needed to provide services [31]-[32].

3.2 Connectivity, Compatibility and Longevity

3.2.1 Connectivity

Although the vast number of devices in the IoT network are to be linked in the future, this may

contradict with the current structure of the communication protocols and the underlying technologies. Presently, the communication architecture mostly relies on the centralized client-server paradigm to connect the different nodes of the network and so far the authentication and authorization seem sufficient for the current ecosystem of IoT involving hundreds or thousands of devices. But, when there will be billions of devices to join the network, the brokered centralized structure will be required, which in turn becomes the bottleneck for performance and unauthorized activities. These systems would require a tremendous investment in maintaining cloud servers to manage large-scale sharing of information and then all of the systems will go down regularly if the server goes down or is inaccessible. It is projected that future IoT will be based on a decentralized paradigm and cloud servers shall have the responsibilities of gathering and analyzing the enormous sensed data. Other solutions may involve the use of a peer-to-peer communication model, where devices can identify and authenticate each other directly and can exchange information without involving brokers. This decentralized model will have its challenges, especially in terms of security, but that can be met with emerging technologies, such as blockchain technology.

3.2.2 Compatibility

IoT involves different technologies with varied compatibilities, which makes it difficult for any procedure to compete for becoming standard. It requires extra hardware and software to connect the devices. The other compatibility issues are from the non-unified services of the cloud, diversities of operating systems and firmware and lack of standard M2M protocols among the IoT devices.

3.2.3 Longevity

The persistence of the technologies used to create Cloud-IoT systems is essential for the smooth functioning of the deployed systems. In the next few years, some of these technologies will eventually become redundant, potentially rendering the nodes that implement them useless or ineffectual. This is mainly important, as compared to generic devices of computing having a life span of few years, appliances of IoT (like TVs, smart fridges,…etc.) tend to remain in service for much more longer and should be functional even if the manufacturer of theses gadgets goes out of services [32]-[34].

3.3 Standards

The technological standards that are used for the proper functioning of devices and to deliver services effectively include data collection standards, networking protocols, communication standards and the procedures used for handling, processing and storing of data obtained from servers. This type of aggregation is to increase the data value by increasing the scope, scale and frequency of data available for analysis. The challenges in standardization include developing standards for unstructured data handling, leveraging new tools of aggregation by technical skills. The structured type of data, for example, is stored in the relational database and queried through MySQL. However, the unstructured data is stored in different types of databases consisting of NoSQL without any standard approach of the query. In terms of technical skills, companies often face the challenges of shortage of talent to make strategy, plan, execute and maintain the systems to leverage unstructured big data [17].

3.4 Security

The fast progressions made in IoT technology are changing lives by connecting a vast number of user gadgets to the internet and thereby controlling them remotely. Along with different applications, such as e-health applications based on Cloud-IoT, frameworks are more efficient and offer better services to the users. However, the usage of Cloud-IoT-based systems demands high security of the data that lies within Cloud-IoT infrastructure, as it involves user's private data. Security and privacy have never been as vulnerable as these are currently, with a vast number of systems sending and receiving immense amounts of information wirelessly. Therefore, researchers must focus on developing and enhancing existing privacy and security solutions for Cloud-IoT-based frameworks; for example, schemes of automatic identification, watermarking, active smart-monitoring and verification of fingerprint schemes [35]. Among the various security issues, one of the important and concerning challenges is to minimize IoT node resources that are consumed by security protocols and to reduce the security vulnerabilities, attacks and threats. Another essential security issue is to provide the rules for authorization and the polices to ensure that sensitive data is accessed only by authorized users,

which is pivotal to maintain the privacy of users, particularly when there is a need for integrity to be guaranteed. Data integrity is concerned as the vital element that affects not only the quality of services, but also the majority of security and privacy issues related to it, such as outsourced data, legal aspects, large scale, monitoring and performance. Additionally, several other issues exist, such as lack of trust, location of physical data and information concerning Service Level Agreements (SLAs) when IoT applications are moved to the cloud. The leakage of information can also happen due to multi-tenancy, which can result in unauthorized effects. Furthermore, key-based cryptographic algorithms, such as public-key algorithms, cannot be applied to IoT devices because of the imposition of constraints in their processing power, battery capacity and memory. Specific attention to the growing challenges is also required; for example, there is a possibility of new attacks, such as SQL injection, cross-site scripting, session hijacking and side-channel attacks, to occur. Moreover, there is much vulnerability that includes virtual machine escape and session hijacking, which are problematic to Cloud-IoT infrastructure [35]-[36]. These issues need to be addressed before the Cloud-IoT paradigm will be fully implemented and adopted by the general user group.

4. SECURITY AS A RESEARCH ISSUE IN CLOUD-IOT

Among the research issues discussed above, security is pivotal, because the connected devices having internet connectivity monitor the user devices continuously, which may harm user privacy if that data is leaked to unauthorized users. A large amount of personal data is generated by smart IoT devices; therefore, users need to know that their information is secure and safe and the business has legal responsibilities to keep information secure. IoT systems facilitate the association of both large and small frameworks together and utilize the internet for communication. Users want to be sure about the security of their IoT gadgets before adopting them fully in their usage. IoT frameworks are inherently vulnerable to outside attacks, because the IoT systems use conventional networks to connect everything wirelessly. Researchers are actively working to find viable solutions for many security and privacy issues in Cloud-IoT systems; however, these issues need further investigation, so that user privacy is not compromised [35]. The various security issues that arise in Cloud-IoT include the common and important issues of Confidentiality, Integrity, Availability of sensed data and the Authentication of devices and data itself. Cloud-IoT is a growing technology and is not much more developed to overcome many issues yet, including security. There is much importance of security when developing the solutions of Cloud-IoT, as there are possibilities of many attacks to happen in the development phase. Without addressing security issues properly, users hesitate to adopt the Cloud-IoT technology in their day-to-day life, as it can harm their privacy; for instance, in a smart health care system that needs to have time-to-time valid data of patients for their continuous observation and if this data is damaged by attackers, this can cause serious outcomes, such as wrong medication leading to the death of a patient. Similarly, in smart homes, personal data may be breached for any harm, intelligent transportation may be hijacked to cause accidents, …etc. Security in Cloud-IoT is a core issue that needs to be addressed, because the private data available at the cloud or in-transit to the cloud from IoT devices can be exploited by hackers, leading to unauthorized effects.

4.1 Threats to Security and Privacy in Cloud-IoT

The integration of IoT and cloud brings a lot of vulnerabilities due to the involvement of user-specific miniature devices and associated limitations. Privacy preservation is always a fundamental human right and in a business context. It is said to be a protection of customer information to use it more appropriately. The security and privacy of the information used in case of business entities need to follow the application laws, policies, standards and the process by which personal information is being managed. In this notion of security, it is referred to as information security defined by ISO 27001 standards for the preservation of confidentiality, integrity and availability (CIA) of information. Non-repudiation, reliability, accountability can also be deliberated as need-based security [38]-[39]. Some of the most common threats to security and privacy are illustrated in Figure 4 [40]-[41]. The brief descriptions of these threats are presented below.

4.1.1 Threats to Security

Communication Threats: The communication channel may be abused by attackers and intruders to launch various attacks. The following threats are likely to occur in this category:

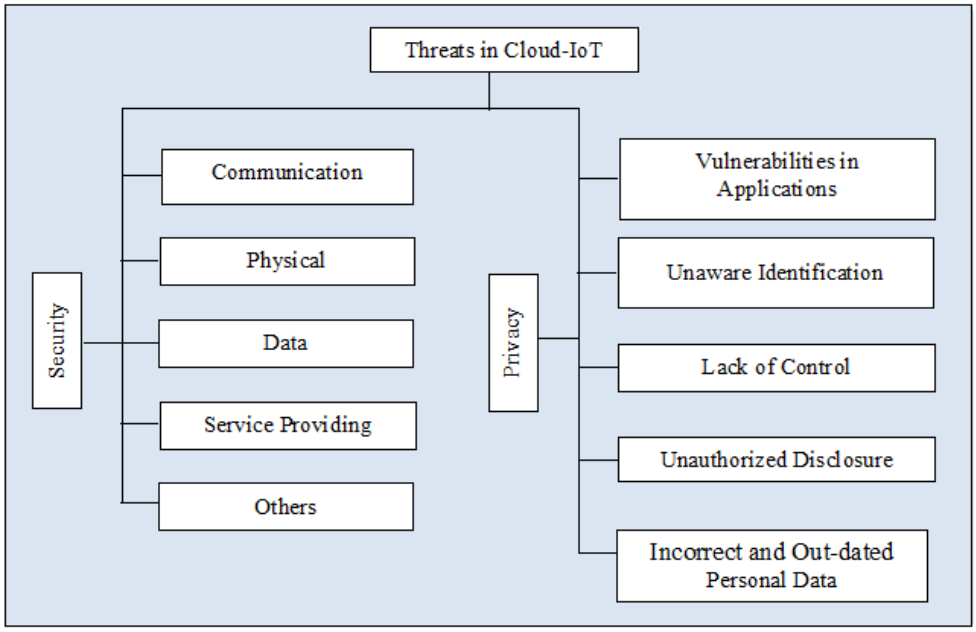

Figure 4. Security and privacy threats in cloud-IoT [40].

a) Denial of Service: Denial of Service (DoS) can be launched over the Cloud-IoT infrastructure in order to reduce the execution of the expected functional capacity of the network, through resource exhaustion, hardware failure and software bugs. DoS attacks are more prominent to the IoT devices in Cloud-IoT infrastructure because of the inherent resource limitations in these devices.

b) Eavesdropping: It refers to the interception of private communications by unauthorized users in real time. Attackers can gain access to the communication channel in order to overhear the secret communication among different network entities.

c) Spoofing Attack: It is an attack where an attacker impersonates and pretends to be an attacker to gain access to restricted and privileged services and bypass existing security and authentication mechanisms. This attack is usually a starting point for a more impactful attack, in most cases, a DoS attack. Such attacks are common to internet-connected devices and therefore make an important attack scenario in the Cloud-IoT system as well which needs to be addressed [41]-[44].

d) Man-in-the-Middle Attack: It is the common cybersecurity attack that establishes security credenti-

als with the sender by impersonating itself to be the receiver. The sender expects to be communicating with the receiver device; however, the information exchange is happening with the attacker that is present between sender and receiver. The attacker then sends the altered messages to the receiver.

e) Replay Attack: This attack relies on an insecure network, in which the attacker captures the data packets and then forwards them at a later time to produce unauthorized effects at the receiver device. The transmission of data is interrupted or replicated by the malicious party, who intercepts the data and retransmits it. A replay attack is possible on a communication protocol when data freshness is not provided. Thus, the network could be secure with respect to authentication, confidentiality and integrity, but does not provide data freshness to mitigate replay attacks.

Physical Threats: These refer to the incidence of harming the devices physically to damage the network devices, resulting in the loss of system and information. The following attacks can be launched under this category:

a) Device Capture: The attackers can capture legitimate IoT devices in order to extract the information held in these devices before it has been transmitted to the secure system for storage. The attackers can also extract the security keys and the shared secrets at IoT devices. The legitimate IoT devices are destroyed by damaging their radio-module and by deleting their memory, which can result in severe damage to Cloud-IoT infrastructure.

b) Node Damaging: Having easy access to physical devices, an attacker can damage any of them physically, which makes them unable to sense and transmit the data. DoS attacks can also be launched

if more devices are damaged by an attacker, so that the entire Cloud-IoT system will become useless and incapable of providing any type of services.

Data Threats: Data threats are considered as common threats for every internet user. The most common threats are: spams, disabling security settings, data corruption and data stealing. The following are the likely threats under this category:

a) Threats during Retrieval, Transfer and Storage of Data: If an attacker gets physical access to an IoT device, then he/she can access the raw sensed data available at devices using micro-probing or reverse engineering techniques. Usually, Cloud-IoT needs to transfer the data at IoT devices to the cloud for storage and processing; therefore, there is a greater risk of data tampering during the transfer of data to the cloud [45].

b) Unauthorized Device Deployment: The attackers can deploy their own devices in the network and send false or infected data to the cloud, resulting in corrupting the entire data that is stored at the cloud. Therefore, the establishment of device authenticity in Cloud-IoT systems is mandatory and if any device fails to prove its authenticity, the data from that device shall not be accepted.

c) Data Loss and Leakage: Events happening accidentally, such as fire, deletion of data by the service provider, earthquakes, …etc. causing loss of critical data. The data can be leaked to unauthorized users accidentally, which can be protected by encryption mechanisms.

d) Data Breach: In this attack, the data can be accessed by unauthorized entities from inside or outside of the system. All types of Cloud-IoT data do not have the same level of sensitivity, as some financial data is more sensitive than other publicly available data and therefore needs to be more protected.

Provision of Service Threats: In Cloud-IoT, many services are used to ensure the operations to happen smoothly, but the threats related to them include the following:

a) Unidentified Users: Services provided by the cloud must ensure that unidentified and unauthorized users cannot gain access to the data being sensitive or not; otherwise this may result in corrupting or authorization of the entire Cloud-IoT infrastructure [42].

b) Identity Theft: In this attack, attackers can access the services and resources, which were otherwise restricted to the user, by gaining access to the credentials of valid attackers that can make the victim accountable for the attacker's actions [46].

c) Compromising Interfaces: It is considered in the top threats of Cloud-IoT, because the APIs are always distributed by the cloud providers to help consumers retrieve data and get access to other services. If the interfaces are not well protected, the attacker can easily get their weakness to be exploited and so -by attacker's data- launch fraudulent services [45]-[47].

Other Threats: Various other threats are not related to the defined categories and some of them are presented below:

a) Malicious Insider: In Cloud-IoT systems, sometimes the attacker having valid authentication and authorization credentials may harm or attack the secret information at network devices by perpetuating the malicious activity on the network. This way, he/she can exploit the access to abuse services.

b) Shared Technology: In Cloud-IoT systems, there exist several shared resources that can be used remotely. Using the shared resources through virtualization can allow access of other Virtual Machines (VMs) of other users, which occurs due to vulnerabilities in VM monitor that may be exploited by malicious users to gain access to the other valid users' VMs.

c) Cloud Computing Abuse: The biggest advantage of cloud computing is that a user can have huge computing power available that is allowed by the organization, which can assist malicious users to get an opportunity to launch varied attacks. A single attacker can even get many resources of computing on-demand to launch a DoS attack to other cloud service providers [48].

4.1.2 Threats to Privacy

The evolution of Cloud-IoT emerges new ways of interaction that concern various privacy and security issues based on technologies and features that are used to deliver Cloud-IoT services. Many

threats can be exploited to harm the privacy of users in Cloud-IoT systems. Some of the likely threats are presented below:

a) Vulnerability in Applications: If companies do not consider the vulnerabilities in delivering the application patches or even complete applications, the hackers or attackers can exploit these vulnerabilities to enter the system and create unauthorized effects.

b) Unaware Identification: IoT devices can be used to collect user data without their knowledge, which can be achieved by using undisclosed small-sized cameras or sensors in users' devices or surrounding areas. The data collected can be used to identify the user and his/her associated attributes, which is the real threat to user privacy [39].

c) Lack of Control: Once the data is collected and uploaded on the cloud, sometimes it is possible to have either limited access or no access to it and in other words, it can be said that the control over data is sometimes lost. The ubiquitous process of sense makes it difficult for users to give their consent to collect data or the actions to be performed after the collected data has been processed and analyzed. Additionally, it becomes a challenging task to create rules for access control to protect privacy. To have keen attention to the preservation of privacy in any system, consent is considered as a major requirement for the collection, storage and processing of personal information [49].

d) Unauthorized Disclosure: The use of cloud infrastructure might impact the users when cloud providers experience difficulties to get the consent about user data collection and processing which may result in unauthorized disclosure of sensitive data.

e) Incorrect or Out-dated Personal Data: It is to be resolved if there is any out-dated or incorrect data in the system; for instance, a patient in an e-health system has been diagnosed with some illness which gets cured after some time. If this kind of information is not updated in the database, the treatment in accordance with the previous report will be harmful to the patient. Similarly, companies should maintain data accurately and update it frequently.

5. STATE-OF-THE-ART SECURITY MECHANISMS IN CLOUD-IOT

The security of Cloud-IoT systems depends on the type of application they are used in. For example, in a smart home application, the security of the latter relies on various things, such as the security of the devices themselves, the security of the wireless infrastructure where these devices are connected (e.g., the home Wi-Fi network), the security of the wired network that connects the smart home to the Internet and the security of the cloud service that the homeowner is subscribed to. Similarly, in e-health application, the security of such a system depends on the security of network infrastructure where medical sensors are deployed, the mobility of patients, the cloud service to which patients and doctors are subscribed to, the security of the medical sensors and the devices that doctors use to monitor and prescribe medicines to patients and the security of network infrastructure through which electronic health records are exchanged. In all applications of Cloud-IoT systems, the user data needs to be protected from attackers and thus, the security solutions are developed so that the sensitive data is protected from attackers. The IoT security solutions involve the secure architecture of multiple levels that use important features of security in IoT across four different layers which are briefly defined below:

a) Device Level Security: Device level security refers to the hardware level solutions of IoT. The security components in this level include chip security, secure booting, device identity and authentication and physical security.

b) Communication Level Security: Communication level security refers to the security of the connection medium through which data is transmitted and received. The security components in this layer include access control, end-to-end encryption, intrusion detection and preventions and firewalls.

c) Cloud Level security: It refers to securing the software backend solution of IoT. Cloud-IoT providers are expected to provide security from major breaches of data itself. The security components in this layer include platform security, data at rest and verification of application integrity.

d) Lifecycle Management Securities: Lifecycle management securities refer to securing the continuous processes that are required to keep the IoT solution's security up-to-date. The security components in this layer include policies and auditing, risk assessment and secure decommissioning.

The security mechanisms based on cryptographic protocols need to play an important role at all levels of security enhancement. The detailed view of security encryption mechanisms and the protocols being used are discussed below.

5.1 Encryption Mechanisms

Most of the components of Cloud-IoT systems, such as IoT devices, storing devices and cloud are vulnerable to different attacks. Attackers can find the location of any network node or device on the network and can easily harm it. These situations can be avoided using encryption mechanisms, such as enciphering the data and its storage location and transferring the encrypted data among devices instead of unencrypted data [50]. Stored data in data warehouses can also be attacked; therefore, the need for strong encryption mechanisms is required. Various secure and popular cryptographic algorithms are implemented for internet security and some of them are shown in Table 3 [51]-[52].

Table 3. Cryptographic algorithms suite [51].

Algorithms	**Purpose**
Rivest Shamir Adelman (RSA), Elliptic Curve Cryptography (ECC), ECDSA	Confidentiality, Digital Signature
Advanced Encryption Standard (AES)	Confidentiality
HMAC, SHA-3, BLAKE-3	Integrity
Diffie-Hellman (DH)	Key Agreement

AES is given the first option of all the standards, as it can be used at all layers of IoT for imparting security, while ECC is viewed as another primitive used at the physical layer, network layer and application layer. The protocols that employ AES as a security construct include Constrained Application Protocol (CoAP), which is used as an application layer protocol for the Internet of Things, Bluetooth-Low-Energy version 4.2 (BLE 4.2), Internet Protocol version 6 (IPv6), 6LoWSec and 4G [53]-[54]. The different security policies are chosen in accordance with the application demands, such as whether end-to-end encryption is required or not. End-to-end encryption provides high-level security, wherein the sender and the receiver can only read the message content and none in the middle can get the message content. In traditional networks, TLS/SSL and IPSec protocols are commonly used to provide authentication, integrity and confidentiality services to communication messages. IPSec is designed to provide security at the network layer either in transport or tunneling mode, whereas the TLS/SSL protocol is used to provide security services at the transport layer. TLS/SSL or IPSec protocols can be used by the applications to access the internet *via* encrypted details of authorized users. Weak APIs and interfaces are attractive attributes for attackers to capture or sniff packets. The most important security construct for users in Cloud-IoT is the availability of network services. A potential attack to availability is the DoS attack, which is launched through the flooding of packets to exhaust network resources. Researchers believe that Cloud-IoT is more vulnerable to DoS or Distributed Denial of Service (DDoS) attacks, as it is shared by many users, which can be reduced by monitoring user requests. Before processing the request, prior identification of undefined requests or duplicated messages shall be erased [51], [55]-[58].

5.2 Different Ways of Handling Cloud-IoT Security

There are different methods to handle the security concerns which mainly rely on cryptographic protocols and some of the ways to handle Cloud-IoT security challenges include:

a) Cloud-IoT security analytics: It involves collecting, correlating and analyzing data from various sources that can help security providers identify threats and nip them up.

b) Public Key Infrastructure use: It includes the set of policies, hardware and software means that are needed for the creation and distribution of digital certificates, which are essential components for various public-key schemes. To be an effective solution for Cloud-IoT security, this method has

proven successful over the years. Some of the Public Key Infrastructure (PKI) methods are used for the management of private or public keys and X.509 digital certificates.

c) Ensuring protection of communication: The communication of sensitive information in IoT needs to be protected from hackers and attackers, which can otherwise lead to unauthorized effects. Cryptographic algorithms, such as AES, ECC and RSA are the most widely used encryption algorithms.

d) Ensuring authentication of devices: Device authentication is essential for ensuring that malicious data is not injected into the network by malicious nodes, which can result in damaging the crucial information in the network. Two-factor authentication, digital certificates and biometrics are the basis of authentication to reduce vulnerabilities.

5.3 Existing Security and Privacy Solutions of Cloud-IoT

The existing security techniques proposed in the literature to ensure security and privacy in Cloud-IoT systems are presented in this sub-section.

Authors in [59] presented that developing confidential infrastructure for Cloud-IoT applications is very expensive in comparison to the low-cost infrastructure of the public cloud, due to the large amount of data generated by IoT. Therefore, more public clouds are used for processing tasks even in case of sensitive data, which leads to increased concern for maintaining the confidentiality of data. One of the ways to mitigate the concern of confidentiality is to encrypt the data at the source and then send it to the cloud for storage purposes only. One of the promising approaches proposed to overcome this bottleneck is Partial Homomorphic Encryption (PHE). In this paper, a scheme for confidentiality preserving continuous query execution in an un-trusted cloud through API initiative that allows programmers to focus on the analysis of automatic homomorphism, the logic of applications and original techniques of compilation, has been proposed. In Zhu et al. [60], the scheme of data integrity is proposed with the combination of ZSS signature and is related to security, privacy and scalability to meet the requirements of computation and storage functions of analytical applications with big data. The remote integrity is implemented while using the ZSS signature. With the use of the ZSS signature, the computational overhead is reduced compared to BLS algorithms. This represents the solution with less overhead in terms of communication and computation than in current RSA and BLS-based data integrity solutions. Authors in [61] proposed a security framework for the Cloud of Things (CoT) that addresses some of the identified security issues in the existing CoT environments. The proposed framework provides several advantages in terms of efficient resource usage, data prioritization, data delivery timeliness and an adequate security level to sensitive data. A confidentiality-preserving system for CoT has been proposed in [62], which uses the Partial Homomorphic Encryption (PHE) mechanism to encrypt the data. The proposed system enables programmers to concentrate on application logic, compilation mechanisms, homomorphism evaluation and optimized resource usage. Authors in [63] have designed a deep reinforcement learning-based malware propagation model. The developed model has been assessed for energy consumption *vs.* number of nodes, average infections over time, node mobility over time period and propagation speed.

In [64], the proposed architecture to achieve availability is ascertained through the execution system based on the Open-STACK. To ensure availability, a template-based cloud framework has been proposed, which can configure fault identification and recovery measures automatically according to different services and features. According to the characteristics and services, proposed method applications were allowed by the templates and the feasibility methods were demonstrated with the existing architecture *via* comparison. In [65], an authentication scheme has been proposed, in which the biometric parameters are combined with the user credentials. The additional key is generated for the ECC algorithm for improving its security level. Normally, in ECC, only two keys are created that are public and private; however, in improved ECC, an additional secret key is generated. This additional secret key achieves the requirements of security, like low encryption, computation and decryption time overhead. Authors in [58] proposed the concept of secure trusted things aiming to reduce the security and privacy concerns in Cloud-IoT systems. It includes an encryption mechanism that involves less overhead. Authors in [66] have proposed a lightweight security scheme for IoT, wherein the energy-efficient and simple cryptographic operations are used. Authors in [67] proposed a security scheme for smart home systems based on Cloud- IoT infrastructure. It proposes group key

management for smart home system. Here, the proposed scheme ensures secure data transfer *via* symmetric key cryptography. The analysis of the proposed security scheme depicts that it is easy to implement, energy-efficient and flexible.

In [68], integration of secure and intelligent security architecture is proposed for the Cloud of Things, in which users are able to access applications in the cloud. Elliptic Curve Cryptographic (ECC) has been used to provide security services. Authors in [65] designed biometric authentication for a multi-cloud sever environment. The core building blocks in their scheme are biometric-based hashing and ECC. In [69], the security and privacy challenges are investigated and discussed by introducing the fog computing in IoT. In this investigation, the authentication issue has been considered as the main challenge with the context of Cloud and Fog computing that is coupled with the applications of IoT. In [68], an adaptable model has been proposed for securing communications in Cloud-IoT systems in contrast to existing pre-configured solutions. It defines the operations of secure communication to agree dynamic and autonomous security protocols and keys of cryptography. Authors in [70] have analyzed the effect of mobility on the authentication and have used Forwarding First (FF) Protocol and Authentication First (AF) Protocol in their analysis. The results depict that mobility affects these protocols in terms of delay and energy consumption. In [57], privacy preserving in message forwarding scheme is constructed for Cloud-IoT systems that are intended to improve efficiency and privacy of transmission. They have developed the architecture of the cloud server having two layers in order to improve the efficiency of communication of clients. In [18], the secure Cloud-IoT method is proposed. The authors conducted the survey based upon the security issues in technologies involved in both Cloud and IoT. After discovering the benefits of cloud and IoT, the authors have surveyed the security challenges in the Cloud-IoT system and proposed a method that improves privacy and security issues in Cloud-IoT. In [72], a list of security solutions, such as the use of private cloud with the parameters of enterprise, session container use, encrypted content and cloud access broker visualization of security at the run-time, have been presented. These solutions are used for different application demands and are expected to improve the overall security of Cloud-IoT-based systems.

6. PRIVACY AND SECURITY OPEN CHALLENGES

It is imperative to manage access, communication and use of available resources of IoT and make efficient protocols and standards for such resource-limited devices. The information that IoT devices gather shall be protected from unauthorized access. There is a need for crucial technologies to protect the individual's privacy and security in the context of Cloud-IoT while having reliable and efficient communication between IoT and cloud infrastructure. It is observed that the benefits of the integration of cloud and IoT have also generated new sets of research challenges. Therefore, there is a further requirement of transformation in technologies of cloud to manage the flow of data and ownership of data source within Cloud-IoT. The data is also accessed by third parties while having virtualization of IoT resources, a new type of interrogations with the regard to data ownership and trustworthiness of data is needed to be addressed. Furthermore, eavesdrop and monitoring of people without their knowledge and consent is another serious problem.

In Cloud-IoT systems, *ad-hoc* connections and backend cloud communication are commonly occurring activities which demand security. Authors in [73] presented that there is a need for an agreement protocol for secure communication that allows the communicating entities to have a mutual agreement based on keys and cryptographic algorithms. In the Cloud-IoT environment, there is a need for adaptable and flexible agreement mechanisms because of storage, bandwidth and computational limitations in IoT. The major obstacles and challenges to practical security in Cloud-IoT systems are given below:

a) Dynamic Cycle of Activity: Different roles and functions can be taken up by connected IoT devices depending on the security challenges in Cloud-IoT systems. The data may be directly transmitted to other devices or cloud servers.

b) Interaction of Heterogeneity: Cloud infrastructure is provided by different manufacturers who use different sets of protocols, technical requirements and standards, which puts hindrances for the interoperability among connected device platforms as well. Because of heterogeneity of the protocols

and technological features of the interconnected devices, it is important to implement new security algorithms in order to ensure safe communication of sensitive data.

c) Provision of Antivirus: Antiviruses are usually used in traditional networks to protect personal computers from attacks and malware. These are memory-consuming and put a great challenge for being used in resource-limited IoT devices.

To make Cloud-IoT a successful technology, various identified research issues need to be addressed by the research community to make Cloud-IoT globally adopted.

7. CONCLUSION

The new and growing technology known as Cloud-IoT or Cloud of Things (CoT) is going to make a huge impact in the future. Both these technologies vary in their characteristics and features but aggregating them together brings several benefits, such as minimization of effort, less costs to incur on hardware, interacting with real-world entities and the like. IoT generates massive data that cannot be stored in IoT device memory or on simple servers; therefore, bringing the cloud into the picture solves big data issues in IoT. On the other hand, IoT assists the cloud to be able to interact with real-world objects. However, the integration of the two technologies brings several research issues that have been highlighted in this paper and the pivotal research issue that has been observed is the security issue that arises due to the amalgamation of cloud and IoT technologies. In this paper, different threats to security and privacy have been identified and the relevant existing security mechanisms have been presented. Further, open security and privacy issues have been identified, which requires further research efforts in order to address these issues. This paper can act as a baseline for research needed in the area of security and privacy issues in the Cloud of Things paradigm.

ACKNOWLEDGMENTS

This research work is funded under the seed grant initiative of the TEQIP-III project currently being implemented at the Islamic University of Science and Technology, Awantipora, Jammu and Kashmir, India.

REFERENCES

[1] K. Lounis and M. Zulkernine, "Attacks and Defenses in Short-range Wireless Technologies for IoT," IEEE Access, vol. 8, pp. 88892-88932, DOI: 10.1109/ACCESS.2020.2993553, 2020.

[2] S. Kumar, P. Tiwari and M. Zymbler, "Internet of Things Is a Revolutionary Approach for Future Technology Enhancement: A Review," Journal of Big Data, vol. 6, Article no. 111, 2019.

[3] O. Mashal, T-Y. Alsaryrah, C-Z. Chung, Z. Yang, W.-H. Kuo et al., "Choices for Interaction with Things on Internet and Underlying Issues," Ad Hoc Networks, vol. 28, pp. 68–90, 2015.

[4] O. Said and M. Masud, "Towards Internet of Things: Survey and Future Vision," International Journal of Computer Networks, vol. 5, no. 1, pp. 1–17, 2013.

[5] F. Firouzi, K. Chakrabarty and S. Nassif, "Intelligent Internet of Things: From Device to Fog and Cloud," Springer, Cham, DOI: https://doi.org/10.1007/978-3-030-30367-9, 2020.

[6] H. F. Atlam, A. Alenezi, R. J. Walters and G. B. Wills, "An Overview of Risk Estimation Techniques in Risk-based Access Control for the Internet of Things," Proc. of the 2nd International Conference on Internet of Things, Big Data and Security, pp. 1–8, [Online], available: https://www.scitepress.org/papers/2017/62926/62926.pdf, 2017.

[7] S. Rabhakar, "Network Security in Digitalization: Attacks and Defence," International Journal of Research in Computer Applications and Robotics, vol. 5, no. 5, pp. 46–52, 2017.

[8] B. Ali and A. I. Awad, "Cyber and Physical Security Vulnerability Assessment for IoT-based Smart Homes," Sensors, vol. 18, no. 3, Article no. 817, 2018.

[9] A.Sanzgiri and D. Dasgupta, "Classification of Insider Threat Detection Techniques," Proc. of the 11th Annual Cyber and Information Security Research Conference, p. 25, ACM, Oak Ridge, USA, 2016.

[10] P. Sethi and S. Sarangi, "Internet of Things: Architectures, Protocols and Applications," Journal of Electrical and Computer Engineering, vol. 2017, Article ID 9324035, pp. 1-25, DOI: 10.1155/2017/9324035, 2017.

[11] T. Qiu, N. Chen, K. Li, M. Atiquzzaman and W. Zhao, "How Can Heterogeneous Internet of Things Build Our Future: A Survey," IEEE Communications Surveys & Tutorials, vol. 20, no. 3, pp. 2011-2027, DOI: 10.1109/COMST.2018.2803740, 2018.

[12] G. Daly et al. "Cloud Customer Architecture for IoT," Cloud Standards and Customer, Council Whitepaper, [Online], Available: https://www.omg.org/cloud/deliverables/CSCC-Cloud-Customer-Architecture-for-IoT.pdf, 2016.

[13] Z. Qureshi, N. Agrawal and D. Chouhan, "Cloud Based IoT : Architecture, Application, Challenges and Future," International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 3, no. 7, pp. 359–368, 2018.

[14] J. Zhou et al., "Cloud Things: A Common Architecture for Integrating the Internet of Things with Cloud Computing," Proceedings of the IEEE 17th International Conference on Computer Supported Cooperative Work in Design (CSCWD), Whistler, BC, pp. 651-657, DOI: 10.1109/CSCWD.2013.6581037, 2013.

[15] I. Odun-Ayo, C. Okereke and E. Orovwode, "Cloud Computing and Internet of Things: Issues and Developments," Proceedings of the World Congress on Engineering (WCE 2018), vol. I, London, U.K., [Online], Available: http://www.iaeng.org/publication/WCE2018/WCE2018_pp182-187.pdf, July 2018.

[16] D. Salvatore, M. Giovanni and P. Antonio, "A Utility Paradigm for IoT: The Sensing Cloud," Pervasive and Mobile Computing, vol. 20, pp. 127-144, [Online], Available: https://doi.org/10.1016/j.pmcj.2014.09.006, 2015.

[17] H. Atlam, A. Alenezi, A. Alshdadi, R. Walters and G. Wills, "Integration of Cloud Computing with Internet of Things: Challenges and Open Issues," Proc. of IEEE International Conference on Internet of Things (iThings) and IEEE Green Comp. and Com. (GreenCom), pp. 670-675, Exeter, UK, 2017.

[18] S. Christos, E. P. Kostas, K. Byung-Gyu and G. Brij, "Secure Integration of IoT and Cloud Computing," Future Generation Computer Systems, vol. 78, no. 3, pp. 964-975, 2018.

[19] F. Alhaidari, A. Rahman and R. Zagrouba, "Cloud of Things: Architecture, Applications and Challenges," Journal of Ambient Intelligence and Humanized Computing, [Online], Available: https://doi.org/10.1007/s12652-020-02448-3, 2020.

[20] M. B. Yassein, I. Hmeidi, A. Alsmadi and M. Shatnawi, "Cloud Computing Role in Internet of Things: Business Community Survey," Proc. of the 11th Int. Conf. on Information and Communication Systems (ICICS), pp. 343-348, DOI: 10.1109/ICICS49469.2020.239533, Irbid, Jordan, 2020.

[21] D. Kelaidonis, A. Rouskas, V. Stavroulaki, P. Demestichas and P. Vlacheas, "A Federated Edge Cloud-IoT Architecture," Proc. of IEEE European Conference on Networks and Communications (EuCNC), pp. 230-234, DOI: 10.1109/EuCNC.2016.7561038, Athens, Greece, 2016.

[22] L.Celic and R. Magjarevic, "Seamless Connectivity Architecture and Methods for IoT and Wearable Devices," Automatika. vol. 61, pp. 21-34, 2020.

[23] T. Bhattasali, R. Chaki and N. Chaki, "Secure and Trusted Cloud of Things," Proc. of the Annual IEEE India Conference (INDICON), pp. 1-6, Mumbai, India, 2013.

[24] S. Kamburugamuve, L. Christiansen and G. Fox, "A Framework for Real Time Processing of Sensor Data in the Cloud," Journal of Sensors, vol. 2015, Article ID 468047, pp. 1-11, 2015.

[25] L. Hou et al., "Internet of Things Cloud: Architecture and Implementation," IEEE Communications Magazine, vol. 54, no. 12, pp. 32-39, DOI: 10.1109/MCOM.2016.1600398CM, Dec. 2016.

[26] R. K. Dwivedi, S. Singh and R. Kumar, "Integration of Wireless Sensor Networks with Cloud: A Review," Proc. of the 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence), pp. 114-119, DOI: 10.1109/CONFLUENCE.2019.8776968, Noida, India, 2019.

[27] S. M. Babu, A. J. Lakshmi and B. T. Rao, "A Study on Cloud Based Internet of Things: CloudIoT," Proc. of IEEE Global Conference on Communication Technologies (GCCT), pp. 60-65, DOI: 10.1109/GCCT.2015.7342624, Thuckalay, India, 2015.

[28] M. Korunoski and M. Gushev, "Evaluating the Scalability of a Big Data IoT Cloud Solution," Proc. of the 18th IEEE Int. Conf. on Smart Technologies (EUROCON 2019), pp. 1–5, Novi Sad, Serbia, 2019.

[29] U. Onoriode and G. Kotonya, "IoT Architectural Framework: Connection and Integration Framework for IoT Systems," First Workshop on Architectures, Languages and Paradigms for IoT EPTCS 264, Electronic Proceedings in Theoretical Computer Science, pp. 1-17, DOI: 10.4204/EPTCS.264.1, 2018.

[30] C. Modi, D. Patel, B. Borisaniya and H. Patel, "A Survey of Intrusion Detection Techniques in Cloud," Journal of Network and Computer Applications, vol. 36, no. 1, pp. 42–57, 2013.

[31] S. Yangui, R. H. Glitho, F. Belqasmi, M. J. Morrow and P. A. Polakos, "IoT End-user Applications Provisioning in the Cloud: State-of-the-Art," Proc. of IEEE International Conference on Cloud Engineering (IC2E), pp. 232-233, DOI: 10.1109/IC2E.2016.43, Berlin, Germany, 2016.

[32] M. Elkhodr, S. Shahrestani and H. Cheung, "The Internet of Things: New Interoperability, Management and Security Challenges," International Journal of Network Security & Its Applications, vol. 8, no. 2, pp. 85-102, 2016.

[33] P. Zdankin and T. Weis, "Longevity of Smart Homes," Proc. of IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), pp. 1-2, DOI: 10.1109/PerComWorkshops48775.2020.9156155, Austin, TX, USA, 2020.

[34] P. Sarwesh, N. S. V. Shet and K. Chandrasekaran, "Energy Efficient and Reliable Network Design to Improve Lifetime of Low Power IoT Networks," Proc. of the International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), pp. 117-122, DOI: 10.1109/WiSPNET.2017.8299731, Chennai, India, 2017.

[35] C. Butpheng, K.-H. Yeh and H. Xiong, "Security and Privacy in IoT-Cloud-Based e-Health Systems: A Comprehensive Review," Symmetry, vol. 12, no. 7, Article ID 1191, 2020.

[36] S. Aguzzi et al., "Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination," Report by European Commission, [Online], Available: https://ec.europa.eu/digital-single-market/en/news/definition-research-and-innovation-policy-leveraging-cloud-computing-and-iot-combination, 2015.

[37] Y. Chen, "IoT, Cloud, Big Data and AI in Interdisciplinary Domains," Simulation Modeling Practice and Theory," vol. 102, 2020, DOI: 10.1016/j.simpat.2020.102070, 2020.

[38] R. Saboori, B. Sharma, N. Kumar and G. Gupta, "IoT-based Healthcare Support Services for Arrhythmia: A Review," Journal of Xi'an University of Architecture & Technology, vol. XII, no. VI, pp. 1035-1039, 2020.

[39] D. M. Donno, A. Giaretta, N. Dragoni, A. Bucchiarone and M. Mazzara, "Cyber-storms Come from Clouds: Security of Cloud Computing in the IoT Era," Future Internet, vol. 11, Article ID 127, DOI: 10.3390/fi11060127, 2019.

[40] A. Adamou et al., "Enabling Privacy and Security in Cloud of Things: Architecture, Applications, Security & Privacy Challenges," Applied Computing and Informatics, Elsevier, [Online], Available: https://doi.org/10.1016/j.aci.2019.11.005, 2019.

[41] A. Sajid, H. Abbas and K. Saleem, "Cloud-assisted IoT-based SCADA Systems Security: A Review of the State-of-the-Art and Future Challenges," IEEE Access, vol. 4, pp. 1375-1384, 2016.

[42] F. Md Sadek et al., "Threat Taxonomy for Cloud of Things," In Book: Internet of Things and Big Data Analysis: Recent Trends and Challenges, Edition 1, Chapter 5, pp. 149-190, United Scholars Publications, 2016.

[43] M. Babaghayou, N. Labraoui and A. A. A. Ari, "EPP: Extreme Points Privacy for Trips and Home Identification in Vehicular Social Networks," Proc. of the 3rd Edition of the National Study Day on Research on Computer Sciences (JERI2019), [Online], Available: http://ceur-ws.org/Vol-2351/paper_67.pdf, Saida, Algeria, 2019.

[44] R. Roman, J. Zhou and J. Lopez, "On the Features and Challenges of Security and Privacy in Distributed Internet of Things," Computer Networks, vol. 57, no. 10, pp. 2266-2279, 2013.

[45] S. Babar, A. Stango, N. Prasad, J. Sen and R. Prasad, "Proposed Embedded Security Framework for Internet of Things," Proc. of the 2nd IEEE International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE), pp. 1–5, Chennai, India, 2011.

[46] C. Modi, D. Patel, B. Borisaniya et al., "A Survey on Security Issues and Solutions at Different Layers of Cloud Computing," Journal of Supercomputing, vol. 63, pp. 561–592, 2013.

[47] D. Catteddu and G. Hogben, "The European Network and Information Security Agency (ENISA): Emerging and Future Risk Programme." Computing, vol. 72, no. 1, pp. 2009–2013, 2009.

[48] Y. A. Hamza and M. D. Omar, "Cloud Computing Security : Abuse and Nefarious Use of Cloud Computing," Int. Journal of Computational Engineering Research, vol. 3, no. 6, pp. 22-27, 2013.

[49] Y. Zhang, D. Zheng, R.H. Deng, "Security and Privacy in Smart Health: Efficient Policy-hiding Attribute-based Access Control, " IEEE Internet of Things Journal, vol. 5, no. 3, pp. 2130-2145, 2018.

[50] Z. H. Hu, "The Research of Several Key Questions of Internet of Things," Proc. of IEEE International Conference on Intelligence Science and Information Engineering, pp. 362-365, Wuhan, China, 2011.

[51] H. Suo, J. Wan, C. Zou and J. Liu, "Security in the Internet of Things: A Review," Proc. of the International Conference on Computer Science and Electronics Engineering, pp. 648-651, DOI: 10.1109/ICCSEE.2012.373, Hangzhou, 2012.

[52] A. Alsaidi, "Security Attacks and Countermeasures on Cloud-assisted IoT Applications," Proc. of IEEE International Conference on Smart Cloud, pp. 213–217, NY, USA, 2018.

[53] K. N. Pallavi, V. R. Kumar and S. Srikrishna, "Comparative Study of Various Lightweight Cryptographic Algorithms for Data Security between IoT and Cloud," Proc. of the 5th International Conference on Communication and Electronics Systems (ICCES), pp. 589-593, DOI: 10.1109/ICCES48766.2020.9137984, Coimbatore, India, 2020.

[54] I. K. Dutta, B. Ghosh and M. Bayoumi, "Lightweight Cryptography for Internet of Insecure Things: A Survey," Proc. of the 9th IEEE Annual Computing and Communication Workshop and Conference (CCWC), pp. 0475-0481, DOI: 10.1109/CCWC.2019.8666557, Las Vegas, NV, USA, 2019.

[55] D. Kishore Kumar, G.Venkatewara Rao and G.Srinivasa Rao, "Cloud Computing: An Analysis of Its Challenges & Security Issues," Int. J. of Computer Science and Network (IJCSN), vol. 1, no. 5, 2012.

[56] X. Wang, Z. Ning, M. Zhou, X. Hu, L. Wang, B. Hu, R.Y. Kwok and Y. Guo, "A Privacy Preserving Message Forwarding Framework for Opportunistic Cloud of Things," IEEE Internet of Things Journal, vol. 5, no. 6, pp.5281–5295, 2018.

[57] S. Sharma, M. A. R. Shuman, A. Goel, A. Aggarwal, B. Gupta, S. Glickfield and I. D. Guedalia, "Context-aware Actions among Heterogeneous Internet of Things Devices," US Patent App., 14/187,156, 2014.

[58] A. Hameed and A. Alomary, "Security Issues in IoT: A Survey," Proc. of the International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT), pp. 1-5, DOI: 10.1109/3ICT.2019.8910320, Sakhier, Bahrain, 2019.

[59] P. Eugster, S. Kumar, S. Savvides and J. J. Stephen, "Ensuring Confidentiality in the Cloud of Things," IEEE Pervasive Computing, vol. 18, no. 1, pp. 10-18, DOI: 10.1109/MPRV.2018.2877286, 2019.

[60] H. Zhu et al., "A Secure and Efficient Data Integrity Verification Scheme for Cloud-IoT Based on Short Signature," IEEE Access, vol. 7, pp. 90036–90044, 2019.

[61] F. Daneshgar, O. A. Sianaki and A. Ilyas, "Overcoming Data Security Challenges of Cloud of Things: An Architectural Perspective," Conference on Complex, Intelligent and Software Intensive Systems (CISIS 2019), Part of the Advances in Intelligent Systems and Computing, vol. 993, Springer, Cham, DOI: 10.1007/978-3-030-22354-0_58, 2020.

[62] P. Eugster, S. Kumar, S. Savvides and J. Stephen, "Ensuring Confidentiality in the Cloud of Things," IEEE Pervasive Computing, vol. 18, pp. 10-18, DOI: 10.1109/MPRV.2018.2877286, 2019.

[63] K. Mwangi, M. Shedden and J. Mandu, "Modelling Malware Propagation on the Internet of Things Using an Agent-based Approach on Complex Networks," Jordanian Journal of Computers and Information Technology (JJCIT), vol. 6, no. 1, pp. 26-40, 2019.

[64] Y. Hyunsik and K. Young, "Design and Implementation of High-availability Architecture for IoT-Cloud Services," Sensors, vol. 19, no. 15, Article ID 3276, 2019.

[65] M. A. Khan, S. Member and M. Y. Khan, "A Secure Framework for Authentication and Encryption Using Improved ECC for IoT-based Medical Sensor Data," IEEE Access, vol. 8, pp. 52018–52027, 2020.

[66] B. Adil and M. Ajaz, "Securing Communication in MQTT-enabled Internet of Things with Lightweight Security Protocol," EAI Endorsed Transactions on Internet of Things, vol. 3, no. 12, Article ID 154390, DOI: 10.4108/eai.6-4-2018.154390, 2018.

[67] B. Alohali, M. Merabti and K. Kifayat, "A Secure Scheme for a Smart House Based on Cloud of Things (CoT)," Proc. of the 6th IEEE Computer Science and Electronic Engineering Conference (CEEC), pp. 115–120, Colchester, UK, 2014.

[68] T. D. P. Bai and S. A. Rabara, "Design and Development of Integrated, Secured and Intelligent Architecture for Internet of Things and Cloud Computing," Proc. of the 3rd IEEE International Conference on Future Internet of Things and Cloud, pp. 817–822, Rome, Italy, 2015.

[69] S. Kumari, X. Li, F. Wu, A. K. Das, K.-K. R. Choo and J. Shen, "Design of a Provably Secure Biometrics-based Multi-cloud-server Authentication Scheme," Future Generation Computer Systems, vol. 68, pp. 320–330, 2017.

[70] A. Alrawais, A. Alhothaily, C. Hu and X. Cheng, "Fog Computing for the Internet of Things: Security and Privacy Issues," IEEE Internet Computing, vol. 21, no. 2, pp. 34–42, 2017.

[71] V. Valter, A. Aleksandar, P. Krešimir, M. Miljenko and Z. Ivana, "Adaptable Secure Communication for the Cloud of Things," Journal of Software: Practice and Experience, vol. 47, no. 3, pp. 489-501, 2017.

[72] K. Sundus and I. Almomani, "Mobility Effect on the Authenticity of Wireless Sensor Networks," Proc. of IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), pp. 286-292, DOI: 10.1109/JEEIT.2019.8717497, Amman, Jordan, 2019.

[73] B. Alohali, "Security in Cloud of Things (CoT)," In Book: Cloud Security: Concepts, Methodologies, Tools and Applications," IGI Global, pp. 1188–1212, DOI: 10.4018/978-1-5225-8176-5, 2019.

ملخص البحث:

في هذا العصر، الذي يوصف بعصر الاتصال والتشبيك، فإنّ إنترنت الأشياء تضيف الى المجالات التكنولوجية الموجودة وتجلب ثورة الى عالم تكنولوجيا المعلومات. وتتكون إنترنت الأشياء من أجهزة متصلة ببعضها البعض، قد تكون أجهزةً رقميةً أو ماديةً أو ميكانيكيةً مزودة بمحدِّدات فريدة ولها القدرة على إرسال المعلومات المحسوسة الى أجهزة أخرى بصورة مستقلة. وتُميَّز إنترنت الأشياء على أنها مؤلّفة من أجهزة مقيَّدة المصادر من حيث كفاءة المعالجة وسعة التخزين ومصادر الطاقة. ولمواكبة هذه المحدِّدات، يمكن استخدام التكنولوجيا القائمة المعروفة بالحوسبة السّحابية لتسهيل نظام إنترنت الأشياء عبر تخفيف متطلباته فيما يتعلق بالمعالجة والتخزين.

في هذه الورقة، تمت مناقشة ضرورة دمج السحابة وإنترنت الأشياء والفوائد المتأتّية من هذا الدمج. إضافة الى ذلك، تمّ تحديد عدة قضايا بحثية تنشأ من الدمج المشار إليه. من بين هذه القضايا، لوحظ أنّ المخاوف من غياب الأمن او الخصوصية هي من القضايا المحورية الناجمة عن دمج إنترنت الأشياء والحوسبة السّحابية، التي تحتاج الى معالجة لجعل الدمج ناجحاً. لقد جرى تحديد التهديدات المتعلقة بالأمن والخصوصية ، كما تم بحث آليّات الأمن القائمة في هذه الورقة.

من ناحية أخرى، تسلط الورقة الضوء على القضايا البحثية المفتوحة المرتبطة بالأمن والخصوصية في الأنظمة التي تقوم على دمج إنترنت الأشياء والحوسبة السحابية. ويمكن لهذه الورقة أن تكون أساساً للبحث الذي تبرز الحاجة اليه في مجال قضايا الأمن والخصوصية في مثل هذه الأنظمة (سحابة الأشياء CoT).