SECURE AND RELIABLE COMMUNICATION BETWEEN CLOUD AND IOT SYSTEMS: A REVIEW

Veena Antony, D. Shanmuga Priyaa*

Abstract

As IoT technologies develop and are adopted in various industries, IoT devices with limited resources are challenging the development. Integration of IoT technologies with cloud computing platforms can extend their capabilities. Hence, a new world of computing has emerged called IoT-Cloud or Cloud-IoT. So that IoT technologies are protected from resource constraints, data is collected using IoT technologies and devices is processed and stored on cloud platforms. When The Internet of Things (IoT) uses sensors in a cloud - IoT environment, the data collected from sensors are stored on the cloud platform. Real-time event checking is possible with this type of environment since it is highly extensible. IoT sensor data must not be leaking during communication because some cloud IoT applications are very crucial. The result is the emergence of new classes of security and privacy concerns. This paper mentions the secure and reliable communication between Cloud-IoT Systems.

Keywords: Cloud Computing, Internet of Things, Security, Privacy, Authentication.

I INTRODUCTION

Essentially, cloud computing provides network access to a large shared pool of configurable computing resources that can be rapidly provisioned and released whenever needed with minimal resource management[1]. As part of cloud computing platforms, cloud service providers manage a large amount of computing resources like hardware, CPU, storage, software, etc. They provide different services in the form of infrastructure, platform, and software to the users over the Internet as per their requirement. Its advantages are low initial capital investment, rapid provisioning, scalability, low disaster recovery costs, pay-per-use, etc. Consequently, it has been adopted by enterprises.

Cloud computing has opened up limitless possibilities for businesses and other organisations in the last years in conjunction with the development in Big Data, IoT, etc. Also called the Internet of Everything (IoE), it is a network of things. The IoT mostly relies on cloud computing due to the limited computing capacity of smart products. As the sensor collects a large amount of data, it is stored in the cloud storage server; additionally, cloud vulnerabilities directly affect security and reliability of the IoT. Users must verify the integrity of remote data stored in cloud computing and IoT infrastructure. Parallel to this enormous growth there arise security aspects as well. A shortage of resources can lead to problems with IoT systems in terms of, storage, transmission and processing. The Internet of Things (IoT) can be defined as a network of smart objects and sensors. IoT applications include wearable devices, smart controls in vehicles, smart homes, industries.

IoT-based applications have become an inseparable part of our daily lives. In scenarios involving cloud-based IoT applications, the cloud platform is mainly used to store the data received from the sensors. To maximise cloud computing capabilities, IoT's must be interconnected physically or virtually with cloud platforms. Users of cloud computing - IoT encounters challenges in information security and communication [2].

Department of Computer Science,
Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India
*Corresponding Author

The paper is organised as follows, Section 2 presents the Cloud services and deployment models, Sections 3 is a discussion about the role of IoT in Information and Communication Technology, Section 4 is an in-depth analysis of secure communication between IoT and Cloud systems, and Section 5 presents open research issues and concludes the paper.

II CLOUD SERVICES AND DEPLOYMENT MODELS

A. Service Models

The Three Types of Cloud Computing Service Models are as follows:

i) Software as a Service (SaaS). Using a cloud infrastructure, users can make use of applications provided by the provider. Depending on the client device, the application can either be accessed through a web browser or an application interface. Users do not have control over the basic cloud infrastructure, such as the network, servers, operating systems, storage, or even the ability to configure individual applications, except for those settings that relate specifically to their usage.

ii) Platform as a Service (PaaS). With cloud infrastructure deployment capabilities provided by the provider, clients can use the programming languages, services, libraries, and other tools supported by the vendor. Unlike the underlying cloud infrastructure of the host environment for deploying applications, the user does not manage and control its servers, operating systems, or networks. Instead, the user can manage the implemented applications and configure setting for the application hosting environment.

iii) Infrastructure as a Service (IaaS). In essence, clients are provided with any operating system or application can be deployed and run arbitrary. Processing, networks, storage and other computing capabilities are provided to the client. It is not the user's responsibility to manage and control the specific cloud infrastructure. However, he does have some control over storage, operating systems and deployed applications, and sometimes he can even tweak selected networking protocols.

B. Deployment Models

The four deployment models are as follows:

i) Private Cloud: An enterprise can decide to manage the cloud by itself or take the services of a third party. The third-party cloud service provider may implement the private cloud within the organisation's premises or in its data center. The most notable advantage of a private cloud is that it offers better and direct control over sensitive data as well as the hardware used. Other advantages of a private cloud are the easy moving of data into the cloud due to better proximity and enhanced security levels.

ii) Public Cloud: This utility model of Cloud Computing provides quick access to a shared infrastructure, storage, and other computing resources. These shared resources are hosted in a remote data center, and multiple clients can gain access to them using the internet. Scalability and cost-effectiveness are the major advantages of a public cloud.

iii) Hybrid Cloud: As the name implies, a cloud that is a combination of two or more clouds (private cloud, public cloud and community cloud) is called a hybrid cloud. Workloads can be moved between private and public clouds in a hybrid cloud environment based on changing computing needs and costs. This allows improved flexibility and more options when it comes to data deployment.

iv) Community Cloud: A community cloud is primarily used by a group of people or organisations. It is a

collaborative effort, and the hardware infrastructure is mutually shared by two or more organisations from a specific community. It could either be managed or hosted internally within an organisation in the community or by a third-party cloud service provider. The infrastructure costs are shared among the community members based on mutual agreements [3].

III INTERNET Of THINGS IN ICT

The Internet of Things has the characteristic of objects in an IoT world having to be instrumented and then interconnected before they can be wisely processed and used anywhere, anytime, and however they like., which are the 5A (anytime , anyway ,anything, anywhere, anyhow) and 3I (intelligent instrumented, and interconnected) characteristics[4].

Four pillars from fig 3.1, nurture the ability of IoT to operate successfully: device, data, analytics, and connectivity. In conjunction with best practices, networking methodologies and middleware platforms, the Internet of Things is the glue that binds the four pillars together. As a result, all the physical assets can be connected to a common infrastructure, and an established methodology for gathering machine data can be employed to determine what that data means. When the Internet of Things can work behind the scenes and share a common platform, like a cloud platform, it will only have the power to be truly successful, which is not possible if companies need to maintain multiple and independent systems at the same amount of time.

The four pillars of the Internet of Things are as follows:

A.M2M: The Internet of Devices

It is often referred to as M2M, or machine-to-machine communication, and it is, as the name suggests, two machines talking to one another, or exchanging data, without the need for human interaction. The Internet of Things (IoT) in the industrial sector includes serial or power line communications and wireless communications. M2M communication has been greatly improved by moving to wireless technology and more applications now have the ability to connect.

B. RFID : The Internet of Objects

Utilising technology such as RFID and radio data communications, the Internet of Things actually establishes the Internet by connecting things by utilising the computer Internet. Therefore, one of the essential core technologies of IoT lies in RFID. It is possible for things to operate independently within this network without relying on any human intervention in the process. The RFID system consists of RFID readers and tags, already known as RFID software / RFID middleware, both of which provide the functionality of the RFID system. RFID tags can be passive, or semi passive and active. RFIDs that are passive do not use batteries, while an RFID that is active keeps its signal broadcasting constantly. There is a significant difference between RFID technology and the other three types of IoT technologies in the sense that RFID tags are applied to “inanimate” objects like pallets or animals and these tags are not “intelligent”.

WSN: The Internet of Transducers

As part of the Internet of Things (IoT), Wireless Sensor Networks (WSN) are used to create a network of spaces dispersed with sensors that measure and record the environmental conditions and transmit such information to an internet-based device. WSNs evaluate environmental conditions like sound, humidity, pollution levels, temperature pressure, etc. due to the expansion of WSN, Wireless Sensor Networks, recent technological advancements have opened up the possibility of WSAN, Wireless sensor and actuator networks, that are able to observe physical conditions, process the data, make observations lead to decisions, and perform right actions. An ad hoc network can serve as an essential component of countless systems and can be used for a number of goals,

including battle front surveillance, monitoring of the microclimate inside buildings, detection for nuclear, biological, chemical warfare and the automation of our homes.

C. SCADA: The Internet of Controllers

An IoT wireless sensor network (WSN) consists of a number of sensors that are dispersed geographically and assist in monitoring, recording, and transferring environmental data to an internet server via a wireless network. Wireless sensor networks evaluate environmental conditions including temperature, noise, humidity and pollution levels. It is predicted that SCADA systems will dominate the controls-IT convergence, as the key technology. SCADA, or supervisory, control, and data acquisition systems, refers to industrial control systems (ICS): computers that monitor and control factory-based processes. In a top-layer business system, a SCADA may be an additional layer. Traditionally, SCADA systems are client/server systems. The new wave of technology has made C/S SCADA systems into three-tiered open systems web-based and supported by middleware.

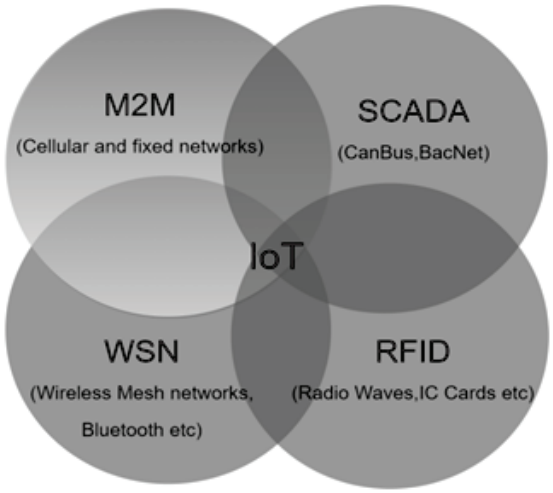

Fig: 3.1 Four pillars of IoT and related networks

IV SECURITY CHALLENGES IN CLOUD –IOT ENVIRONMENT

IoT cloud technologies are multifarious, cloud services, operating systems, and network protocols from many vendors, so they can be difficult to combine, leading to limited portability and interoperability [5]. Additionally, cloud elasticity and scalability are essential in the implementation of the IoT- cloud. The IoT- cloud provider's resources may not be adequate to handle the heightened demand for IoT technologies if they cannot meet the demands for the services. [6].

Now, let us consider the various applications domains and compare the security threat and communication channels in IoT based on the Fig 5.1. In Smart environments, the network communications like Wi-Fi, Zigbee, Bluetooth, LTE, etc, are used among buildings and people face various security challenges in authentication and privacy. Smart grid applications using Wi-Fi, Zigbee, Z-wave, which use IoT devices like smart meters and readers, are prone to eavesdropping, tampering, and physical attacks. Similarly, the applications in health care which use the network communication channels like Bluetooth and Zigbee for connecting IoT devices like sensors and smart wearable devices face privacy breaches and denial of service attacks. Intelligent transportation systems based on IoT devices such as EFC, RSU, OBUs are vulnerable to jamming, congestion, and security breaches.

The main cause of data security issues in smart home technology results from the transfer, storage, and processing of data in clouds owned by someone who is not part of his network. A data breach or loss of data is examples of potential security issues related to data. Loss of data about consumers is caused by data being damaged due to circumstances beyond their control. On the other hand, a data breach is when a person non-authorised steals consumer data without their permission or knowledge. Smart device data is transferred to

cloud-based IoT services through wireless networks that provide open access to the cloud. The consumer does not have access to the data, so it is important to be aware, and cannot control the data in their possession; there is a risk that unauthorised individuals may access the offloaded content. It is not unlikely that another incident will occur in which the integrity of data is compromised later on when the processing of the data occurs in the cloud.

V SECURE COMMUNICATION BETWEEN CLOUD-IOT: A REVIEW

Cloud computing and IoT come from totally different worlds. Although their features are reciprocal, their integration is seen in literature as being beneficial to both due to their reciprocal natures. Numerous lightweight authentication schemes have been proposed over the past few years as a solution to the problem of security vulnerabilities.

Marilyn Wolf and Dimitrios Serpanos define a threat model for safety/security in Cyber-physical systems(CPSs) and IoT systems. CPSs and IoT systems are more secure and safe with these emerging techniques. For CPSs and IoT systems to achieve optimum safety and security, new techniques must be applied both at design time and during the implementation phase, together with the diligent application of existing best practice standards [7]. Mustafa A. Al Sibahee offers low complexity secure End to End(E2E) Smart to Smart message delivery function, by implementing a significant assurance factor like a one time bio key with MAC-SHA-1 through random mapping and by implanting the totality of MAC-SHA-1 in a minimum complexity cover image through double-stegging based on DWT steganography to conserve authentication of messages and data integrity. By providing responsive mutual authentication resulting from such a negotiation process, the known attacks can be prevented. It is also possible to ensure that the measurable cost of the real-time system is very less by using Lightweight Message Delivery between the smart devices, which can satisfy the security needs of E2E communications [8].

A simple authentication scheme based on the IoT is implemented. Many attacks can be avoided and key security features such as the security of session audits, mutual authentications, and user authentication are ensured, therefore it meets the requirements of security resists widely known attacks. The scheme can prevent general attacks and provide features such as obscurity for users and authentication for mutual use, which are essential. It is also proposed methods to upgrade IoT authentication for cloud computing, analyse performance measures for good computation, and have good security properties [9].

With the implementation of Light Weight Authentication Mechanism-Cloud IoT, an authenticated user can remotely access the data from IoT sensors. As part of LAM-CIoT, a structured one way cryptographic function is used in conjunction with a “bitwise XOR operation” (bitwise XOR operation). Also, a fuzzy extractor mechanism is being deployed at the user’s end for local biometric/realistic authentication to turn their investigation into fact. LAM CIoT is methodically analysed for its security ,which is done using the widely used Real Or Random (ROR) model, formal verification of security using AVISPA, an automated security evaluation tool, and informal security analysis. Comparing LAM-CIoT to the closely related schemes of authentication, the performance analysis shows better security, less communication overhead, and low computation overhead. [10].

Nawaf proposes a model that gives benefit in securing the unification of the two different technologies. This model utilise Block chain network, mining nodes and transaction, that are located both in the cloud and on premises. The nodes may include standalone computers, smart devices and enterprise servers. IoT devices with insufficient resources act

as Block chain clients. Such resource of smart devices interacts with upstream cloud based Block chain transaction nodes through Application Program Interfaces [11]. A scheme to both encrypt and search outsourced data in cloud-enabled IoT is presented with an identity based encryption scheme with a tested authorised equivalence , IBE-AET. According to IBE-AET, an authorised cloud server is allowed to conduct an equivalency test on a message encrypted using the same identity as well as a message encrypted with a different identity. As an added benefit, IBE-AET utilises a versatile authorisation mechanism which allows users to delegate testing capability in a fine-grained manner to the cloud server. AET becomes equivalent to Diffie-Hellman in the random oracles model [12].

Despite the widespread adoption of sensor-cloud solutions, most solutions do not provide opportunities for authenticating nodes and measuring data security in the context of malicious threats that compromise the trustworthiness of networks. From the data presented in this section, it can be concluded from the aforementioned results that the sensor cloud infrastructure can be applied to large-sized regions within a network to increase the network's scalability and availability. In developing a solution, it may be necessary to consider the limitations of low power sensor nodes. Thus, the proposed solution's is to provide a secure and authentic cloud-based sensor architecture to improve data gathering and energy efficiency. A major benefit of the proposed architecture is that, it can provide a lightweight cryptosystems, which can be measured in terms of CIA triads (confidentiality, integrity, and authentication). Further, the proposed architecture optimises the computational oncosts on the sensor nodes by integrating cloud and sensor networks with minimal energy consumption [13].

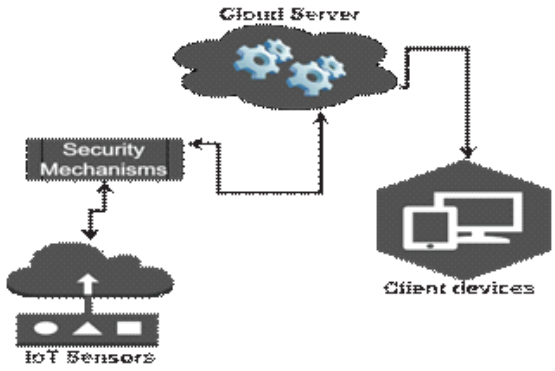

Fig 5.1: Security in IoT-Cloud Platforms

Analysis and design of heterogeneous network resource management algorithms are based on information security transmission, and its advantages .A calculation based on the resource management algorithm on information security transmission is performed to realise the design of the paper by establishing a resource management model and implementing a heterogeneous network resource management algorithm. As an example of an intelligent method for the collection, coding, and transmission of pest and disease data. Using the secure transmission of information to manage the resources could reduce calculation errors and improve security because the algorithm relies on the safe transmission of information. The algorithm error is reduced by twenty percent whereas the performance of security is above ninety percent. In this sense, the algorithm proposed in this paper improves the management quality significantly when calculating resource management in heterogeneous networks, reduces resource management failures, increases algorithms' efficiency, and verifies the proposed algorithm's effectiveness and practicality [14].

Using an identity-based encryption, an IoT user can encrypt data to share data with a recipient by using a flexible privacy-preserving data sharing scheme ie: FPDS scheme. A

significant feature of this architecture is that the IoT user can set a policy and then use this delegation credential to send all the ciphered data, which satisfies the access policy to the cloud, creating new cypher texts that a new recipient can access. Users of IoT can use the cloud to share and secure their data in this way without violating their privacy. An in-depth analysis of the security issues of FPDS shows that the scheme can be used by semi-trusted cloud and malicious IoT users [15]. Data in the cloud and on IoT devices must be verified for integrity and availability prior to being stored in them. There are currently a variety of remote data integrity verification schemes, most of which rely on RSA and BLS signatures. The RSA based scheme has too much computational expenses. The BLS signature based scheme requires a certain hash function, and it has low signature efficiency when used in big data environments. The authors propose a verification scheme for data integrity based on a short signature algorithm , ZSS signature, which will address the existing signature procedures' computational cost and signature efficiency issues. The introduced trusted third party (TPA) will provide additional privacy protection and public auditing. It is possible to significantly reduce the computational overhead by reducing the overhead associated with hash functions. It is known that, assuming CDH's difficult problem is considered, it can protect against adaptive chosen message attacks. Using this scheme it results in greater efficiency and safety [16].

As a result of the AES algorithm, a key setup time of about two seconds can be achieved for good key agility with a fast setup time. As a result, this algorithm could be used to implement a trusted relay algorithm using an encryption of the speed key for use in the Decode and Forward (DF) model. The implementation of DF and Amplify and Forward (AF) methods, instead of the use of trust relays, has few serious weaknesses in the AES encryption and can be utilised in the integrated new model to benefit security. As an added benefit, the implementation of AES requires less memory, so it is suitable for environments with limited memory. It can thus take advantage of the transmit power that the AF model provides when transmitting, resulting in a more reliable and trustable transmission. This model is designed to extend the advantages of the Internet of Things and Cloud Computing by developing a platform that enables scalability and innovation in delivering secure and private services [17].

As items are moved through cloud platforms, IoT storage allows for tracking of valuable information about those items. IoT applications gain significant benefits by being able to gain insights into how IoT data is currently processed, which results in higher availability and flexibility of resources. A data storage system supporting IoT devices provides a major competitive advantage for IoT applications by improving the overall data processing efficiency. A semantic relationship between IoT data and other data sources will lead to greater inter-operational capability (contextual business scene, semantic annotation, multi-device, etc.) and global intelligence. Enterprises will be able to acquire such capabilities through IoT data storage systems [18].

The architecture of an cloud-IoT platform has been presented for the integration of IoT and cloud technologies. There are five main components to the proposed software platform: An interface between the cloud and the device, data management, authentication and a cloud to user interface. Cloud to device interfaces serve as an interface for transmitting data among cloud platforms and their IoT devices. As part of setting up data transmission, the communication interface interacts with the authentication component to ensure that the IoT device will be sending the data to the cloud is a legitimate device. Registering an IoT device through a web console component enables valid IoT devices to be part of the cloud system. A data storage component collects the sensor data. In addition to storing data, various data processing components can be used to

analyse it. The API-based access to data and the web console allow users to retrieve the collected data, whether raw or processed. In order to satisfy the communication, security, and storing requirements, the proposed system has been functionally tested. Moreover, we find that the number of concurrent device connections has an impact on the time required for sensor data to reach the cloud and the speed with which it is received from IoT devices [19].

Albert Guan has proposed a protocol of key agreement with authentication capabilities to enable the establishment of session keys in wireless networks between two communication nodes. Based on the volatility of noise in the communications channel, the protocol's security is based on. In this sense, the protocol does not guarantee computational security, but rather information security. Due to the noise present in the communication channel, it is possible for the eavesdropper to detect different types of message received by the two communication points as well as by the eavesdropper themselves. In order to increase the reliability of the encryption, the developers devised a method for resolving the mismatch between the two communication nodes, after which the common bit string can be used to extract the secret session key. Since the eavesdropper may use information he gains from observing the execution of the protocol, it is demonstrated that the common string shared by the two communication nodes must be uncertain. They have shown that the eavesdropper cannot learn the secret session key shared between the two communications nodes [20].

VI CONCLUSION

Cloud computing and the Internet of Things have become highly interconnected over the past few years. IOT enabled by the cloud is expected to promote the development of what is known as ‘digitalisation’ in human society and increase the level of intelligence. A new scheme for data integrity checking is proposed in this paper to address the issue of data security in cloud and IoT systems. With this scheme, we fully consider security, scalability, and privacy protection to meet the demands of computing, storage methods and communication for the Internet of things, to support large amounts of aggregated data for analysis. It does not apply to multi-replica environments in which data integrity verification is required. As a result, we will next investigate a real-time and multi-copy data integrity verification scheme.

Future research should focus on cryptographic security methods that can better operate on resource-limited IoT devices through Crypto Clouds. Users with varying levels of technology experience will be able to successfully use and implement IoT systems despite the lack of consumer interfaces on many of these IoT devices. Furthermore, the collection and sharing processes that are done by the connected IoT devices are in need of standardisation in order to ensure that they are operating at peak levels. Using such a standard will reduce the number of unforeseen vulnerabilities and the associated attacks upon platforms that are not homogeneous.

REFERENCES

[1] P. Mell and T. Grance, The NIST Definition of Cloud Computing, September, 2011, National Institute of Standards and Technology (NIST), Information Technology Laboratory.

[2] Z. A. Abduljabbar, H. Jin, A. Ibrahim, Z. A. Hussien, M. A. Hussain, S. H. Abbdal, and D. Zou, “Privacy-preserving image retrieval in IoT-cloud,” in Proc. IEEE Trustcom/BigDataSE/ISPA. Hong Kong: IEEE Press, Aug. 2016, pp. 799–806.

[3] Aws Naser Jaber and Mohamad Fadli Bin Zolkipli,”Use of Cryptography in Cloud Computing.” 2013 IEEE International Conference on Control System,

Computing and Engineering, 29 Nov. - 1 Dec. 2013, Penang, Malaysia.

[4] Honbo Zhou,"The Internet of Things in the Cloud,"Version Date: 2012918 International Standard Book Number-13: 978-1-4398-9302-9.

[5] Darwish, A., et al., The impact of the hybrid platform of internet of things and cloud computing on healthcare systems: Opportunities, challenges, and open problems. Journal of Ambient Intelligence and Humanized Computing, 2019. 10(10): p. 4151-4166.

[6] Malik, A. and H. Om, Cloud computing and internet of things integration: Architecture, applications, issues, and challenges, in Sustainable Cloud and Energy Services. 2018, Springer. p. 1-24.

[7] Marilyn Wolf and Dimitrios Serpanos, "Safety and Security in Cyber-Physical Systems and Internet-of-Things Systems",Vol. 106, No. 1, January 2018 | Proceedings of the IEEE,106(1), 9–20. doi:10.1109/JPROC.2017.2781198.

[8] M. A. AL Sibahee et al.: "Lightweight Secure Message Delivery for E2E S2S Communication in the IoT-Cloud System",IEEE Access,Volume 8, 2020.

[9] Hsiao-Ling Wu , Chin-Chen Chang , Yao-Zhu Zheng , Long-Sheng Chen and Chih-Cheng Chen ,"A Secure IoT-Based Authentication System in Cloud Computing Environment", Sensors 2020, 20, 5604; doi:10.3390/s20195604.

10] Mohammad Wazid , Ashok Kumar Das , Vivekananda Bhat K, Athanasios V. Vasilakos,"LAM-CIoT: Light weight authentication mechanism in cloud-based IoT environment", Journal of Network and Computer Applications (2019), doi: https://doi.org/10.1016/j.jnca.2019.102496.

[11] Nawaf Almolhis, Abdullah Mujawib Alashjaee, Salahaldeen Duraibi and Fahad Alqahtani,"The Security Issues in IoT- Cloud: A Review", 2020 16th IEEE International Colloquium on Signal Processing & its Applications (CSPA 2020), 28-29 Feb. 2020, Langkawi, Malaysia.

[12] Rashad Elhabob,Yanan Zhao, Nabeil Eltayieb, Abdeldime M. S. Abdelgader and Hu Xiong,"Identity-based encryption with authorised equivalence test for cloud-assisted IoT", Cluster Computing https://doi.org/10.1007/s10586-019-02979-1(0123456789().,-volV)(0123), Springer 2019.

[13] Khalid Haseeb , Ahmad Almogren ,, Ikram Ud Din , Naveed Islam and Ayman Altameem ,"SASC: Secure and Authentication-Based Sensor Cloud Architecture for Intelligent Internet of Things",Sensors 2020, 20, 2468; doi:10.3390/s20092468.

[14] Ding Li , Wang Zhongsheng , Wang Xiaodong and Wu Dong,"Security information transmission algorithms for IoT based on cloud computing " ,0140-3664/© 2020 Published by Elsevier B.V.

[15] Hua Deng , Zheng Qin, Letian Sha and Hui Yin,"A Flexible Privacy-Preserving Data Sharing Scheme in Cloud-assisted IoT",DOI 10.1109/JIOT.2020.2999350, IEEE Internet of Things Journal .

[16] HONGLIANG ZHU , YING YUAN , YULING CHEN , YAXING ZHA , WANYING XI , BIN JIA, AND YANG XIN,"A Secure and Efficient Data Integrity Verification Scheme for Cloud-IoT Based on Short Signature",Digital Object Identifier 10.1109/ ACCESS.

2019.2924486.

[17] C. Stergiou, K. E. Psannis, B.-G. Kim, and B. Gupta, "Secure integration of IoT and cloud computing," Future Gener. Comput. Syst., vol. 78, pp. 964–975, Jan. 2018.

[18] H. Cai, B. Xu, L. Jiang, and A. V. Vasilakos, "IoT-based big data storage systems in cloud computing: Perspectives and challenges," IEEE Internet Things J., vol. 4, no. 1, pp. 75–87, Jan. 2017.

[19] Bhawiyuga, A., et al., "Architectural design of IoT-cloud computing integration platform". Telkomnika, 2019. 17(3)

[20] Albert Guan,"A Lightweight Key Agreement Protocol with Authentication Capability",DOI: 10.1142/S01290541215002