GE-International Journal of Management Research
ISSN (O): (2321-1709), ISSN (P): (2394-4226)
Vol. 10, Issue 10, October 2022 Impact Factor: 7.466
© Association of Academic Researchers and Faculties (AARF)
www.aarf.asia,**Email** : editor@aarf.asia, editoraarf@gmail.com

Internet of Things : Innovation in Cloud Services and Security Architecture

Devarshi Chatterjee

Student, Indian Institute of Management Nagpur, India

deva.chat123@gmail.com; 9748362579 (M)

and

Prof (Dr) Devapriya Chatterjee

Ex-Director (MBA), Shankara Group of Institutions Jaipur,

Management Consultant and Chartered Engineer (India)

chatterjee.devapriya@gmail.com;9123999144 (M)

Abstract

Organizations would manage multi-domain and cross-organizational deployments of IoT across trust boundaries. Big Data aspects of the IoT, that require security, would benefit from the innovative cloud services and security architecture. The data analytics, reporting systems, and data storage of IoT are the main guiding factors for securing these innovative services. The elements of security, that are the responsibilities of the customers, and of the cloud providers, need to be addressed. The paper reviews and identifies the external and the internal security threats, that are related to IoT, and delves into innovative cloud-based offerings and security controls. The paper explores a few cloud service providers, along with their software and security features. The paper also examines the building of an innovative IoT enterprise security architecture by studying the security functionality needed from the cloud. The paper further explores the available offerings of the cloud security, to mold into an efficient IoT cloud security architecture. New computing paradigms, poised to be delivered by cloud, are also exhaustively discussed. The paper discusses the innovative IoT systems and data coupled with cognitive analytics, in cases of collaborative navigation techniques and positive health monitoring.

Key Words : analytics, cloud-based, deployments, multi-domain, and paradigms

Introduction

The cloud is the optimum mechanism for the tracking of the state and the location of the IoT devices. The IoT cloud services support firmware updates, configuration control and device provisioning as well. The security provided by the cloud services is of utmost importance, considering the ability of these services to directly influence the security and functional state of an IoT device. If the attacks on the cloud services are compromised, it would be necessary to make changes on a large scale, to the state of many IoT devices simultaneously. The ability to track inventories and assets is an important aspect of IoT security. The cloud is the solution for IoT inventory and asset management, and provides a view into the authorized and registered devices, operating within the boundaries of the organizations. The IoT devices, offered by the vendors, for services, require the capability of preparing the billing in response to usage, as well as the ability to authorize device operations and track entitlements. Cloud applications provide real-time monitoring abilities, when used in support of mission-critical roles. Several functions, like, industrial monitoring and industrial control systems, are being ported to cloud by organizations for enhancing the availability of data, opening up new customer services, and, reduction of operational costs. The cloud plays a central role in making workflows automated, and enable IoT services to gather the latest instructions, information and restrictions. Programmable Logic Controllers and Remote Terminal Units are devices that support the ability of monitoring IoT systems more effectively and efficiently, and become directly connected to the cloud. These new functions are enabled by Representational State Transfer communications.

Objectives

The main objective of the research is to utilize the security functionality of the cloud to build the security architecture of an IoT enterprise by :

a) Updating firmware and software
b) Authenticating security controls
c) Making recommendation for end-to-end security
d) Ensuring the maintenance of data integrity
e) Enrolling and bootstrapping of IoT devices
f) Monitoring of IoT security

Methodology and Data Collection

The cloud-based security offerings were studied at length for collection of data, and video-conferencing was made with the specialist IoT managers of Azure IoT suite of Microsoft, IoT platform of IBM Watson, Amazon Web Service IoT and Fog Computing of Cisco.

It transpired from Azure IoT suite of Microsoft that the IoT device management comprises of powerful features like automatic configuring and updating of firmware and software, that enables IoT per device configuration, along with IoT device-level topology management, that assists in establishing group-level control of access, management and permissions. The device group Application Programming Interface, provides the group management service, and the registry management Application Programming Interface, provides software versioning, management features and provisioning. Centralized authentication is provided by using the existing authentic framework. The cloud to device and device to cloud communication are enabled through IoT related protocols. The suite provides to developers through a generic IoT Hub message format, the cross-protocol fusion capabilities. The IoT Hub enables cloud to device communication, and device to cloud communication by supporting IoT related protocols. There are various entry points for connected devices, into the cloud. The Azure Content Development Network is a tool used to distribute firmware updates to the IoT device inventory.

It came to light from IoT platform of IBM Watson that the following IoT interfacing capabilities are included in the foundational IoT Application Programming Interfaces :

a) Updating, viewing and registering devices
b) Operation in ingested and historical datasets
c) Viewing of the organization’s IoT devices and inventory

The computing ability of the system to solve problems from gargantuan ingested datasets is utilized in various industries, like healthcare.

It was observed that Amazon Web Service IoT comprises of the framework to allow the communication of IoT devices with the cloud, using a variety of protocols. The IoT devices can speak in the cloud with each other, through application brokers. The IoT integrates with other services offered by Amazon, that includes the utilization of the real-time data streaming and analytics engine, named Kinesis, that operates a platform for ingestion, accepting streams of data and loading into other domains of Amazon. Amazon Web Service IoT preconfigures the IoT devices and uploads the configurations to the physical devices, at the time of being online. There is an intermediary between the IoT device and the controlling application, known as Amazon Web Service Thing Shadow. This leverages the protocol named Message Queuing Telemetry Transport with topics, that are predefined, and could be used to interact with the IoT devices and service. A JavaScript Object Notation is published for each response and update. The Amazon Web Service IoT suite gives the advantage of the log management integration through CloudWatch, that is a management and monitoring service, and could be configured to log process events on flowing messages, from IoT devices to the Amazon Web Service infrastructure. CloudTrail is a service of Amazon Web Service, that enables compliance, governance and audits. It is leveraged for Amazon Web Service based IoT deployment, to enable analytics, compliance tracking and security analysis.

In Cisco, the main issue of the address of the cloud is the operation of the majority of IoT devices, in a region close to centralized processing by cloud or at the network edge. Cisco's rebranding of the edge of computing is derived from the visible moisture, ie fog, at the ground, and central cloud, ie sky. The feature of having processing and data as edge-central, has the following benefits :

a) Local control and management of policies, that are based on edge conditions
b) Efficiency of network and data projecting that porting the large volumes of data that comprise IoT, for security and application purpose, is difficult due to clogged networks
c) Latency is reduced as data-intensive edge applications for the IoT are real-time, for involving vast amounts of localized decision-making, response and sensor data

The Cisco model is the best in the sense, that reporting and monitoring applications; actuators and controllers; time-sensitive sensor streams, and large datasets are associated with industrial IoT. Fog computing of Cisco is in its early lifecycle, and is implemented in a middleware framework of Cisco, that is known as IOx and is meant for effective IoT technologies. This an application environment, between hardware and applications running directly on edge-equipment. The Cisco DevNet Software Development Kits support IoT Fog Computing development. Cisco cybersecurity solutions, like TrustSec, Identity Services Engine and Cisco NetFlow, are utilized by IoT organizations.

A context of cloud-based IoT is illustrated in Figure-1

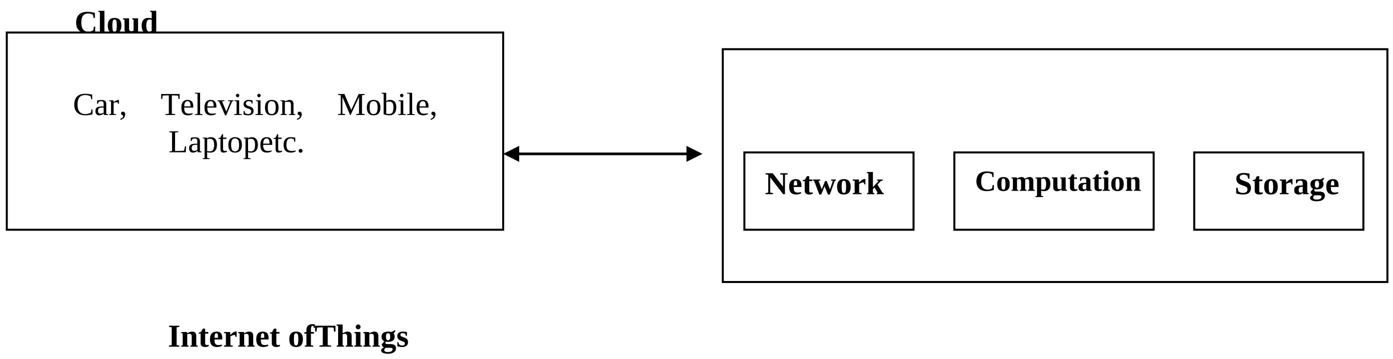

Figure 1 : A Context of Cloud-Based IoT in Communication with Each Other

The IoT threats to cloud-based infrastructures are examined below in Figure-2, for a suitable resolution :

Areas of Threats	Nature of Targets
Applications and networks	Flooding of endpoints is denied, and networking components are virtual
Virtual Endpoints	Misconfiguration of web servers, vulnerabilities of virtual machines and web applications, insecurity of IoT brokers and gateways, vulnerabilities of misconfigured databases for proper access control

Users and administrators of Cloud system	Cross-site scripting of web browsers on host machines of users, downloading of malicious payloads from e-mail attachments and web browsing, that often compromise the organization’s cloud-based enterprise.
Logical and Physical Threats to IoT devices connecting to the Cloud	These include sniffing traffic, as well as tampering or accessing data, missing or theft of IoT devices, poor perfect-forward secrecy and ciphersuites, insecurity of storage-on-device and database, insecurity of gateways of IoT edge, end-point spoofing of IoT devices like redirecting of IoT communication, or improper authorization and authentication, injection and tampering of malicious payloads into the protocol of IoT communication traffic between edge gateways, devices and cloud gateways

Figure-2 : IoT Threats to Cloud-Based Infrastructure

The above comprise of some security topics that need to be considered during the use of or the migration of IoT infrastructures to the cloud. The security risks of the organizations operating IoT systems and devices are lowered by the automated Infrastructure-as-a-Service (IaaS) capabilities of the cloud. The high costs of on-premises security and maintenance are reduced by the security offerings of hosted cloud services and infrastructure, that necessitate fewer cybersecurity professionals. Secure-by-default configurations to networks and Virtual Machines have been consistently applied to the cloud-provisioned IaaS services, that benefit client organizations with economic security practices.

Analyses and Results

We have observed a variety of cloud-based services, supporting the deployment of IoT. The endpoints of each cloud and stakeholder, play vital roles in securing the multitudes of transactions. The Cloud Support Providers, support the basic controls, as authentication and encryption to the cloud. The authentication of the cloud services security controls require :

a) Direct authentication of IoT devices (having security and functional resources) to gateways and brokers
b) Authentication of end users to cloud applications
c) Authentications of the applications of the cloud (including brokers and gateways of IoT) from one to the other
d) Verification of the authenticity for functionaries of administration and Application Programming Interfaces (multi-factor authentication).

We have observed that Amazon Web Service Identity and Access Management is a multi-featured platform for authentication, supporting multi-factor authentication, full integration, federated identity and permission management for users and roles. Multi-Featured Authentication devices could be used by both virtual cloud providers, as well as, by end users. An open standard for authorization is OAuth2.0 (RFC6749), that is used by Amazon Web Service, for allowing secure and delegated access to third-party web servers. OpenID Connect is a service, that is built on OAuth2.0, using identification tokens, acquired through OAuth2.0 transactions, for supporting authorization of users.

Azure IoT suite of Microsoft provides federated identity authentication, as well as its own Active Directory authentication framework. It offers both OAuth2.0 and OpenID Connect identity-as-a-service.

A few end-to-end security recommendations for IoT cloud deployment could be made ;

a) Tagging of data for protection of privacy
b) Obtaining privacy agreements with peer organizations, and making assessment of the adequacy of the security controls implemented by the organizations
c) Making notification on the usage of the data
d) Tracking of the privacy controls by the service providers with information generated by a person, or by a device tied to a person
e) Applying secure configurations to the database, feeding the reporting and analyzing applications
f) Ensuring an integrity protection and end-to-end authentication from cloud service provider to the IoT devices with the gateways as pass-throughs.

g) Providing sufficient protection to the cloud applications, supporting the reporting and analyzing workflows
h) Segregation of devices on customer networks ensuring that tampering is not possible
i) Making application of rigorous software development practices for databases and web services that serve the IoT devices
j) Making application of integrity protections to IoT device data, transmitted from IoT device to the gateway, and gateway to the cloud
k) Making encryption of the data when needed
l) Providing protection against the attacks of denial of service by using properly configured and robust load balancing application gateways
m) Ensuring that the services of messaging and transactions between devices are integrity protected and authenticated
n) Ensuring that the data being transmitted to the IoT devices or gateways is authenticated by the devices themselves

The concept of security of IoT context by trustworthy cloud is illustrated in Figure 3.

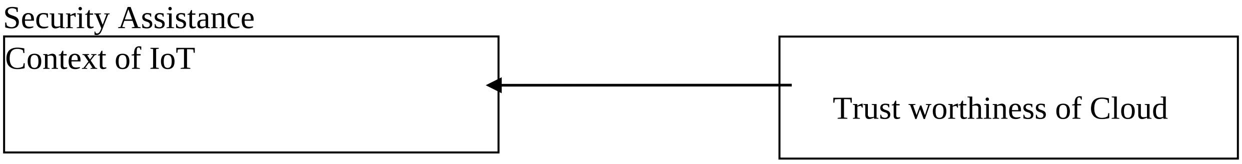

Figure 3 : Security of IoT Context by Trustworthy Cloud

In order to ensure that a high integrity of the data, for usage in enterprise IoT system, is maintained, the following are needed :

a) Application of integrity controls and authentication to IoT devices, for ensuring that fraud devices are unable to transmit data to the cloud
b) Installation of gateway devices and securing of configuration for operation on-site or in the cloud
c) Adopting measures for software security for the web service, that collects data and interfaces with IoT devices and gateways
d) Configuring security infrastructure, that supports the IoT web servers

The configurations of IoT brokers and gateways, need to continuously monitor any malfunction of the endpoints, such as :

a) Scanning of topic
b) Connecting by client but not sending data
c) Terminating connections in an abnormal way
d) Making attempts of connection in a repetitive manner
e) Dispatching messages that are undeliverable

The correlation of the functioning of an IoT device with events occurring in other parts of the system need to be understood. The field of Security Information and Event Management needs to be tuned carefully to identify the potential misuse of IoT systems. Message Queuing Telemetry

Transport brokers need to capture messages from subscribers and publishers for instant notification of malfunctioning. The occurrence of bootstrap at the vendor, depends on the criticality of the concerned IoT device. It needs to be understood that the bootstrap function and the subsequent enrollment, results in the operational status of the IoT devices over a network, in a secured fashion.

Discussion and Finding

It is clear from the research that it would be possible to tailor an IoT cloud security architecture for an enterprise adopter. The choice of architectural aspects and options are large for cloud services in the security architectures of an IoT system. In order to implement the security architectures of cloud services, the IoT service providers, enterprise adopters and cloud service providers initially examine the capabilities that are being provided, for focusing the architectural security controls in the IoT framework. An example of tailored IoT cloud security architecture is illustrated in Figure 4.

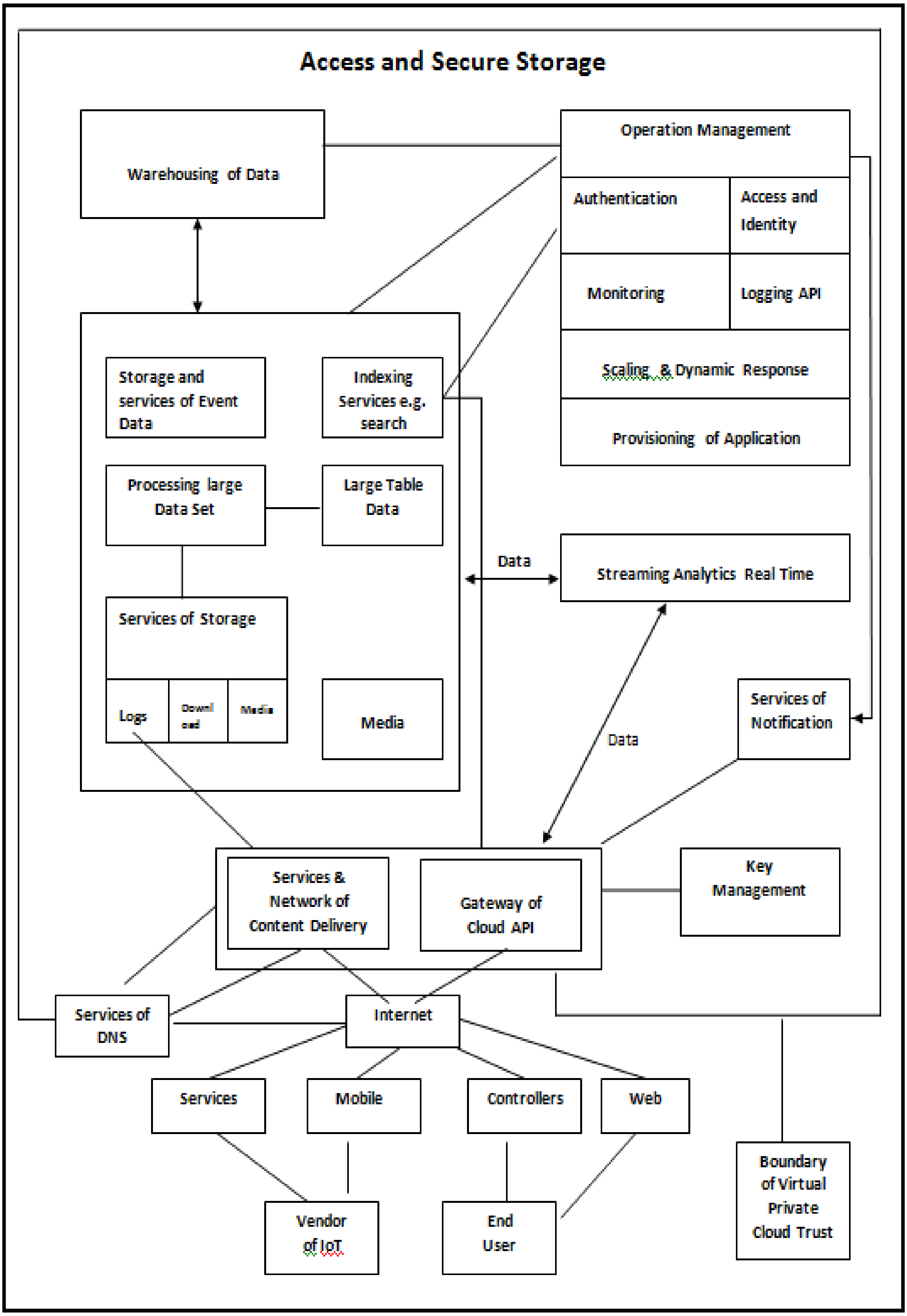

Figure 4 : An example of cloud service provider offering security to an IoT organization

For cloud services leading to the providing of security architecture in IoT deployment, we need to assemble the already available services and the primitive security architecture that are available from the cloud service provider, and then adapt to the innovation. The procedure is briefly discussed here :

a) It is needed to characterize the system and the security starting point by conducting a detailed threat model as follows :

   1. Examination of the North and South protocols, required by the platform of field gateway for transmission and coalescing of communication to the cloud gateway, as well as, to make communication with the field devices
   2. Determination of data protection, storage and reuse, that are needed in transit and at rest
   3. Identification of the logical and physical security characteristics of the system endpoints, along with their authority of administration and control
   4. Categorization as well as identification, that are based on privacy and sensitivity of IoT data, that originate from the IoT devices at the edge of the network
   5. Finalization of the assessment of the privacy and risk against the data, for ascertaining the necessary controls, that are unavailable from the cloud service provider.
   6. Identification of the protocols, types and platforms of the existing IoT devices
   7. Determination of the distant as well as nearby producers of data, along with the consumers of the sensitive data
   8. Determination of the types of data, needing protection point-to-point on the basis of risks, and those that need protection end-to-end, for the guarantee of the integrity, confidentiality and the origin
   9. Ascertaining how people of the organizations, interacting with IoT services and databases, remain enrolled in the system, obtain access and permission, and are audited as well tracked

b) It is needed to formulate a cloud based security architecture of IoT deployment, with the following data :

   1. Adapting and developing procedures and policies pertaining to privacy and security of data, as well as requirements of security, services, and roles of administrator and user
   2. Direct provisioning of security from cloud service provider
   3. Integrating all the practices of security

4. Adding on the security services that are cloud based, and available from cloud service providers, or through third party services, that are interoperable and compatible
5. Integrating and adopting one own cloud-based security structure, into the Application Programing Interfaces and frameworks, that are supported by the cloud service provider

We have thus found from the research that the cloud has many characteristics, that make it an adaptive, enabling and attractive technology, from which we could build, envision and deploy new IoT services. Software Defined Networking is a network of next-generation management capabilities, for reduction and simplification of work for reconfiguration of networks and management of policy-based routes. The network is made more dynamic and programmable, that is necessary for the much-needed flexibility, for managing the global IoT traffic. The architectures of Software Defined Networking function by the decoupling of network control from the functions of forwarding. These comprise controllers of Software Defined Networking, implementing a Southbound Application Programming Interface, and a Northbound Application Programming Interface, connecting network controllers and applications respectively, to the networking devices, that perform traffic forwarding. The benefits of Software Defined Networking are derived by the architectures of IoT, that leverage large cloud services. The security vendors utilize Software Defined Networking for tackling the challenges of distributed denial of service, and it is recommended that enterprises move forward for tailoring their implementations, for supporting that functionality. The cloud environment provides tools that are capable of structuring and managing the data, from the gargantuan quantities of data, that sinks in the IoT.

The diverse nature of IoT hardware platforms is a major challenge in the IoT development environment. There are a variety of platforms with different software development kits, drivers, and Application Programming Interfaces. There are different programming languages, that vary across hardware, that include Python, C as well as embedded C. A flexible development environment, that is also reusable, need to be shared across the development framework. The same is possible through the use of container technology. The technology involves the building of containers with packages and libraries, that could develop the device in use. The containers act as a development baseline, and could be shared and replicated across the development framework. New baselines are created for use, adding new software library stacks, when new types of IoT devices are developed. A development tool, known as Docker, has the best ability to deploy containers, as well as store and manage the workflow of IoT device images. Docker enables system administrators and developers to deploy firmware and software images, directly to hardware. The benefits of Docker include the updating of device images, and integration with a test system, for subjecting the IoT system, to full testing. Google's open source Kubernetes, enables Docker to make the organizations manage the large clusters of containers. IoT deployment is greatly enabled by the distributed computing ability of the easily managed clusters of containers.

It was found that there was a concept of modularizing monolithic and large enterprise applications, into small and bite-sized services, that is known as Microservices. It mitigates and simplifies the complex enterprise applications, with changing requirements of the environment. Microservice architecture is responsible for the formation of self-contained and separately virtualized Virtual Machines, that have their own Application Programming Interface, data backend and business logic, and connect to other microservices. Apart from lending naturally to elasticity of cloud, the microservice architectures simplify long-term maintenance and development, of large and small-scale cloud applications. The cloud architecture is capable of spinning up new microservice containers, for impact on services. Microservice architecture could generate new IoT enterprise applications, in the data-rich environment, and dynamically scale the new services, in response to the ebbs and flows of data processing.

It was further observed that networking through 5G would be the key tool for IoT, to support orders at higher data rates than Long Term Evolution networks. The specifications of 5G, for this purpose, need the following :

a) Reduction of latency under 1 ms
b) Starting date rate of 1GB/s and evolving to multi-GB/s
c) More energy-efficient equipment

Several advanced organizations are making high investments and preparing for big growth, with the availability of IPv6 and the near-future 5G connectivity.

Limitations and Future Scope of Research

The distributed and centralized cloud-processing is pushing the IoT to new directions. We are aware of new services, like Airbnb, Uber and others. On-demand computing is a new delivery model that is significantly made available in cloud-based elastic architectures. These resources are delivered, billed and scheduled on a changing climate demand, and are based on-demand. The inverse of IoT may surpass the huge benefits of the cloud to the IoT. The IoT, with the advantage of 5G, available compute resources, and the large number of edge devices, benefits the applications, that are cloud-based, to enhance the availability to various edge applications, the latent compute resources. On-demand local clouds, that are dynamic and supported by IoT, would find that 5G networks are necessary, and enable the applications that are yet-to-be-imagined. The IoT-facilitated on-demand-computing, along with the network support, would evolve new architectures, like microservices, and their fine-grained execution. The basic requirement of IoT provisioned on-demand computing, is a trusted and secured computing domain, within IoT devices. The cross-domain computing for the IoT, are enabled by new technologies, like TrustZone, that provide the foundation for system-wide security.

The cloud-based service and client endpoints of present days, are secured by Public Key Infrastructure and digital credentials. A new project called Milagro, forms independent and multiple Distributed Trust Authorities, along with pairing-based cryptography, for independent generation of private and multiple key shares to servers and clients. The final crypto-variables, for key agreement and mutual authentication across the cloud environment, are constructed by the consuming endpoints. The success of Milagro might lead to the emergence of new open source distributed trust models, for the cloud and IoT deployments.

It has been observed that IoT is too large for grouping the potential cognitive processing usage cases, into a small set. The horizon with IoT systems and data, coupled with cognitive analytics, portray pictures as given below :

a) Collaborative Techniques in Navigation : These techniques enable Unmanned Aircraft Systems, operating in Global Positioning System denied environment, to understand in a collective fashion, their environment, for more effective navigation
b) Predictive Monitoring of Health : The bio-datasets of massive health monitoring, coupled with metadata of patient in various forms, enable the cognitive systems, to

clerically predict the probability of maladies of health before appearing or disease conditions in general. IoT systems would be the backbone of monitoring of health. For data fusion services, wearables, as well as other private and public data sources, it is observed that cognitive systems would have greater dataset resolutions, with which to identify the health risks.

Conclusion

We expand the use of the available technology, provided in the cloud environments by the integration of the IoT and the cloud. There are, however, several challenges, as with new technologies, being faced by the researchers, with regards to achieving success in IoT environment and cloud-based IoT context. The two most serious challenges for the cloud-based IoT context are trust (misuse of data and malicious nodes) and security (the physical layer access control management). Hence the adoption of the new technology, transfers the trust and security issues of the IoT to the cloud. It has been established by research that a trustworthy cloud ensures the security of the IoT context. The main drawback is the inadequate literature in the trust assessment of cloud-based IoT context, whereas there is abundant literature in the aspect of security of IoT addressed wireless networks. The paper emphasizes on ensuring the security of the cloud-based IoT context, by the assessment of the trustworthiness of the cloud service.

Reference

1. C. Stergiou, K. E. Psannis, B. G. Kim, and B. Gupta, “Secure Integration of IoT and Cloud Computing”, *Future Gener. Comput. Syst.*, vol. 70, pp. 104-125,May 2017
2. *Cloud Computing Service Metrix Description,* Standard, National Institute of Standards and Technology, Special Publication 500-307, Apr. 2018
3. Cloud Security Alliance. (2015). *Cloud Controls Matrix v3.* [online]. Available : https://cloudsecurityalliance.org/research/com
4. H. Kim, “Enhancing Trusted Cloud Computing Platform for Infrastructure as a Service”, *Adv. Elect. Comput. Eng*., vol. 17, no.1, pp. 9-14, 2017
5. H. Ma, Z. Hu, K. Li, and H. Zhang, “Toward Trustworthy Cloud Service Selection : A Time-Aware Approach Using Interval Neutrosophic Set”, *J. Parallel Distrib. Comput*., vol. 96, pp.75-94, Oct. 2016
6. *Information Technology-Cloud Computing-Service Level Agreement (SLA) Framework-Part 3 : Core Conformance Requirements,* Standard ISO/IEC DIS 19086-2, International Organization for Standardization and International Electrotechnical Commission, Oct. 2016.
7. J. Luna, A. Taha, R. Trapero, and N. Suri, “Quantitative Reasoning About Cloud Security Using Service Level Agreements”, *IEEE Trans. Cloud Comput.,*Vol. 5, no. 3, pp. 457-471, Sep. 2017

8. J. Ni, K. Zhang, X. Lin, and X. S. Shen, “Securing Fog Computing for Internet of Things Applications : Challenges and Solutions”, *IEEE Commun. Surveys Tuts.,*vol. 20, no. 1, pp. 601-628, 1st Quart., 2018
9. J. Siegel, and J. Perdue, “Cloud Services Measures for Global Use : The Service Measurement Index (SMI)”, in *Proc. Annu. in SRII Global Conf.,* San Jose, CA, USA, 2012, pp. 411-415
10. M. Tang, X. Dai, J. Liu, and J. Chen, “Towards a Trust Evaluation Middleware for Cloud Service Selection”, *Future Gener. Comput. Syst.,*vol. 74, pp. 302-312, Sep, 2017
11. N. Somu, M. R. Gauthama Raman, K. Kirthivasan, and V. S. Shankar Sriram, “A Trust Centric Optimal Service Ranking Approach for Cloud Service Selection”, *Future Gener. Comput. Syst.*, vol. 86, pp. 234-252, Sep. 2018
12. S. Ding, S. Yang, Y. Zhang, C. Liang, and C. Xia, “Combining QoS Prediction and Customer Satisfaction Estimation to Solve Cloud Service Trustworthiness Evaluation Problems”, *Knowl. Based Syst.,*vol. 56, pp. 216-225, Jan. 2014
13. S. K. Lee, M. Bae, and H. Kim, “Future of IoT Networks : A Survey,” *Appl. Sci.,*vol. 7, no. 10, p.1072, 2017
14. S. Siadat, A. M. Rahmani, and H. Navid, “Identifying Fake Feedback in Cloud Trust Management Systems Using Feedback Evaluation Component and Bayesian Game Model”, *J. Supercomput.,*vol. 73, no. 6, pp. 2682-2704, 2017
15. S. Singh,and J. Sidhu, “Compliance Based Multi-Dimensional Trust Evaluation System for Determining Trustworthiness of Cloud Service Providers”, *Future Gener. Comput. Syst.*, vol. 67, pp. 109-132, Feb. 2017
16. S. Wang, L. Sun, Q. Sun, J. Wei, and F. Yang, “Reputation Measurement of Cloud Services Based on Unstable Feedback Ratings”, *Int. J. Web Grid Services,* vol. 11, no. 4, pp. 362-376, 2015
17. Q. Wang, D. Chen, N. Zhang, Z. Qin, and Z. Qin, “LACS : A Lightweight Label-Based Access Contron Scheme in IoT Based 5-G Caching Context’, *IEEE Access,* vol.5, pp. 4018-4027, 2017
18. Q. Wu, X. Zhang, M. Zhang, Y. Lou, R. Zheng, and W. Wei, “Reputation Revision Method for Selecting Cloud Services Based on Prior Knowledge and a Market Mechanism”, *Sci. World J.*, Feb. 2014, Art. no. 617087
19. T. Halabi and M. Bellaiche, “Towards Quantification and Evaluation of Security of Cloud Service Providers’, *J. Inf. Secur. Appl.,*vol.33, pp. 55-65, Apr. 2017
20. T. H. Noor, Q. Z. Sheng, and A. Alfazi, ”Reputation Attacks Detection for Effective Trust Assessment among Cloud services”, in *Proc. 12th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom),* Jul 2013, pp. 469-476
21. W. Li *et al.,*”System Modelling and Performance Evaluation of a Three-Tier Cloud of Things”, *Future Gener. Comput. Syst.*, vol. 70, pp. 104-125, May 2017
22. X. Li, J. He, B. Zhao, J. Fang, Y. Zhang, and H. Liang, “ A Method for Trust Quantification in Cloud Computing Environments”, *Int. J. Distrib. Sensor Netw.,*vol. 12, no. 2, p. 5052614, 2016
23. X. Li, X. Jin, Q. Wang, M. Cao, and X. Chen, “SCCAF : A Secure and Compliant Continuous Assessment Framework in Cloud-Based IoT Context”, *Wireless Commun. Mobile Comput.,* vol. Oct. 2018, Art. no. 3078272
24. Y. Yang, X. Peng, and D. Fu, “A Framework of Cloud Service Selection based on Trust Mechanism”, *Int. J. Ad Hoc Ubiquitous Comput.,*vol. 25, no. 3, pp. 109-119, 2017
25. Z. Zheng, X. Wu, Y. Zhang, M. R. Lyu, and J. Wang, “QoS Ranking Prediction for Cloud Services”, *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 6, pp. 1213-1222, Jun. 2013