OIC-CERT Computer Emergency Response Team

OIC-CERT Journal of Cybersecurity
Volume 4, Issue 1 (April 2022)
51 - 66

A Comprehensive Reconsideration of Cloud Security Approach

Dr.Mohamed Hamad Al Kuwaiti[1], Talal M. Al Kaissi[2]
[1]Head of Cyber Security, UAE Government
[2]Chief Executive Officer, G42 Cloud, UAE
[1]**Malkuwaiti@ra.ac.ae,** [2]**Talal.Alkaissi@g42.ai**

ARTICLE INFO

Article History
Received 8 Apr 2022
Received in revised form 12 Apr 2022
Accepted 15 Apr 2022

Keywords:
Cloud security, Zero trust, Cloud security framework, cloud security domains, open, collaboration, trusted, digital transformation

ABSTRACT

With rapidly growing migration of business, computation and data into the cloud, cloud security is no longer a new topic and is increasingly playing a more critical role in digital transformation. However, with increasing severe cloud security incidents grabbing the headlines recently, it has become imperative that we need to reconsider how to secure the cloud more effectively based on principles about secure-by-design, and zero trust. In particular, cloud security should not only be treated as a technical problem for both cloud service providers and users. But rather, all corresponding stakeholders need to be involved holistically, particularly regulatory authorities. To further clarify and substantiate this statement, this paper firstly comprehensively review cloud security literature but bearing in mind with a wider consideration with regard to future digital transformation scenarios. Additionally, this paper will also systematically organize cloud security concerns into domains, articulate beneficial cloud security principles and practical recommendations towards achieving a secure, controllable, reliable, collaborative and robust cloud ecosystem.

I. INTRODUCTION

Since the advent of cloud computing (cloud) [5], cloud services have been rapidly growing as the technical enabler for both businesses and individuals. However, with higher cloud usage, the focus on its security has also increased exponentially. Over the past decade, massive efforts have been invested to secure cloud services and the cloud environment, to ensure cloud evolves successfully to become the critical infrastructure of the digital transformation era.

ISSN 2636-9680
eISSN 2682-9266

Although many countermeasures against cloud security risks have shown obvious achievements on securing the cloud, it is impossible to guarantee the assurance of an impenetrable cloud. Furthermore, it is also unavoidable that malicious cyberattacks or misconfiguration would have impacted cloud service providers that have many users. The last decade has witnessed a plethora of severe cloud security incidents [6] [7]. As we know, cloud security issues may cause severe data breaches, causing the cloud providers to bear the load of huge compliance costs. Consequently, it seems that urgent challenge for cloud security is much more than just technical issues. In addition to focusing on the solutions for cloud security, we need to reconsider how to proactively pre-empt these issues from happening by efficient coordination of the already scarce resources. This is because the same security problem may be a common issue for various cloud service providers and users. As such, to address this challenge we should also pay more attention to the entire cloud security strategy at a national or regional level, rather than solely focusing on the efforts to shore up defences of cloud service providers and users because cybersecurity is a team sport; to comprehensively solve the cloud security conundrum we need to bring together the entire ecosystem and its stakeholders together. As a result, this creates a higher level of assurance towards cloud security protection by taking advantage of existing resources, such as best practices and standards, while having cloud security to be continuously controlled, managed and improved at a national level or regional level bringing the entire ecosystem together in a holistic manner.

Towards this end, the principles of security by design, zero trust and team sport should be applied so that stakeholders in the ecosystem, especially the regulatory authorities can optimize cloud security strategies, policies and some other technical specification or framework as the guideline to bring everyone onto the same page. Thus, to precisely address this problem statement, this paper would present deep insights and consideration on cloud security, focusing on key stakeholders, such as governments, cloud service providers and major cloud users. Action points and recommendations would be provided that can be adopted as a foundation for regulatory authorities to establish a common cloud security strategy adopting mutually recognized policies and technical specifications.

In furtherance to the objective of this paper, Section Two will cover a literature review to indicate and highlight our queries. Section Three defines the dimensions that we reconsider issues of cloud security. Then, Section Four will systematically introduce our reconsidered results. Finally, the

last two sections discuss and conclude with some key points and future work.

II. RELATED WORK

Whenever a new technology emerges in cyberspace, cybersecurity concerns will follow immediately, which applies to cloud computing. At the start before 2009, researcher had focused on cloud security and privacy issues through enterprise risk management and compliance lens [1]. In Mather et al.'s book, authors concluded that cloud security involves infrastructure security, data security and storage, identity and access management, security management, privacy audit and compliance. Security as a cloud service was introduced in a forward-looking manner. Similarly, Krutz and Russell [2] also provided a guide to secure cloud computing, which mainly focused on cloud computing fundamentals, cloud software security, risks issues, cloud security architecture and cloud lifecycle security issues. The introduction of widely commercial usage of cloud seen security guidance and risks have been created and analysed. Subsequent cloud security research and development also closely follow these previous steps. A few years later, researchers began to summarize common key cloud security challenges. For example, in 2017, researchers concluded some challenges through surveying existing literatures at that time, such as virtualization, privacy, data storage, etc [3]. At the same time, with the onset of an abundance of cloud security research topics as cloud usage uptick tremendously, researchers began to focus on how to match those identified security issues with proper solutions. In Basu and Bardhan et al.'s work [4], they had conducted a practical and instructive survey to promote cloud security. Also, for some publicly agreed cloud security cases and incidents, there was a consideration of prevention. Tirumala and Nadiu, et al [8] analysed and raised a prevention against account hijacking in cloud environment. Additionally, cloud attacks and sensitive data stored in the cloud are summarized as follow two figures [15], respectively:

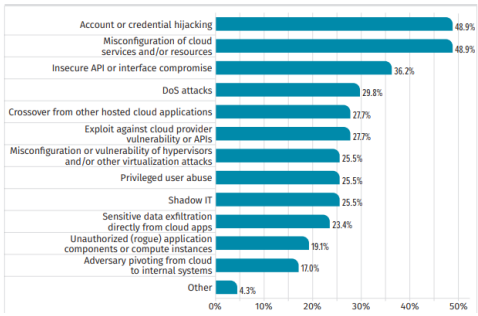

Fig. 1: Breakdown of cloud attack

ISSN 2636-9680
eISSN 2682-9266

Fig. 2: Sensitive data stored in the cloud

Invariantly, with those massive amount of efforts invested into cloud security research, cloud services providers could therefore securely support the cloud as a critical infrastructure and enabler for digital transformation, and user would seemingly enjoy a peace of mind using these cloud services.

Or is that the case? As the cloud matures, more and more business organizations define, specify and indicate cloud security systematically. For example, in [9] and [10], cloud security is generally defined as the composition of data security, identity and access management, policies on threat prevention, detection and mitigation, data retention, business continuity planning, and legal compliance. Then, cloud security scope involves physical networks, data storage, data servers, virtualization, operating systems, middleware, application and terminal device security. As a result, cloud security proposes to enable data recovery in case of data loss, protect storage and networks against data theft, deter human error or negligence, and reduce the impact of any data or system compromise.

Hence, the topic of cloud security either become better defined or the scope has been expanded beyond the elastic limit that once had a well-defined scope of cloud security. Therefore, instead of a reduction in the number of cloud security breaches, we seen the impact and malignancy degree of cloud security breaches growing globally instead [11]. Specifically, we saw LinkedIn fell victim to a data scraping breach in 2021, where 700 million LinkedIn profiles, and the data from the hack was posted on a dark web forum. Additionally, Facebook was also reported some data breaching occurred from 2019, on which user phone numbers, account names and some other personal data was lost. Prior to that, more than half a million Marriott division Starwood's guests' personal data was exposed after a 2018 cyberattack. And forensics indicated that there were compromised networks and system sometimes since 2014 before Starwood's acquisition by Marriott. That means that the problem that we are seeing is just the tip of the iceberg, Virtually, cyberattack has frequently targeted on big business organizations in recent years during the pandemic heralding in a corresponding cyber pandemic [12][32].

Needless to say, it is time for us to reconsider how to address these existing and upcoming cloud

security issues through innovation. In Dubai, UAE cyber security strategy [21], innovation is a main domain to establish a free fair and secure cyberspace. It means dealing with cloud security issues should also rely on such innovation. Obviously, current efforts are not able to defend against security incidents completely and efficiently on cloud. The reason is limited protection sources against cloud attacks are unequally distributed for cloud service providers and users either locally or globally. Clearly, organizations with more influence and resources may implement better protection, compared with those with lesser resources. However, it has been not correct that cloud security should be only responsibility for both cloud service providers and users. Rather, all cloud security stakeholders in the ecosystem should be involved, especially for national or regional regulatory authorities or governmental agencies. This is because the cloud is the critical infrastructure of well-being society and digital transformation, and cloud security has a huge influence on national security as a result. This has motivated certain countries and regions to release a new set of rules and regulations with the inclusion of cloud, such as the EU General Data Protection Regulation (GDPR) [13], and the US Cloud Act [14]. More recently, UAE also enforced a personal data protection law last November, which constitutes an integrated framework to ensure the confidentiality of information and protect the privacy of individuals within the UAE [24]. The Act provides a proper governance for data management and protection and defines the rights and duties of all parties concerned. As a result, it means that cloud ecosystem cannot avoid legal requirements or other compliance considerations. Hence, cloud service providers should consider more data protection measures to ensure compliance to these laws. However, it is more efficient to use a proactive cloud security approach, rather than the outcome-directed cloud security governance. Therefore, a comprehensive cloud security management, technical specification, or a guideline is still missing. As a result, the cloud ecosystem needs to involve more cloud security measures.

By comparison to those cloud security solutions designed for cloud service providers and users, there is much less effort concentrated on the aspect of governmental agency. In next section, for the purpose of establishing a controllable, reliable resilient and secure cloud ecosystem, we would carefully describe how we reconsider cloud security. So that we can eventually realize that a unanimous supervised and governed cloud security framework and we shall be proposing a corresponding working group under OIC-CERT that will be necessary to control, improve and optimize national or regional cloud security in a holistic way. And such

ISSN 2636-9680
eISSN 2682-9266

a framework will focus on assisting national and regional regulatory authorities or governmental agencies to make and implement cloud security strategies, policies technical specification and guidelines.

III. METHODOLOGY

The proposition of such a comprehensive cloud security approach should be a systematic engineering endeavour, and it is required to reconsider cloud security through the following well recognized principles: security by design, zero trust, and team sports.

There are many definitions about security by design, although it was originally defined in software engineering. It means that software products and capabilities have been designed to be fundamentally secure [16]. According to this principle, we need to reconsider cloud security domains initially, more widely. As such, it is recommended that for the following reconsidered cloud security domains that we shall be proposing in subsequent Sections should cover the lifecycle of both cloud service and usage, simultaneously.

On the other hand, with regard to the zero trust principle, although it is an IT-based concept, the vision about "never trust and always verify" has been well accepted globally. It is true that zero trust is more applicable for cloud environment, because data, service, application and servers within the cloud can be easier approached than that in the IT system. As a result, verification should be adapted for the cloud environment. For instance, all users regardless of whether they are in or out of the organization's network, are to be always authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data, while utilizing cloud based in-depth intelligence and analytics to detect and respond to anomalies in real time.

In addition, cloud security should be a team-sport. The dependence of national, regional and global economies on the cloud, has have made it a 'utility' comparable in importance to that of what water, power and telecommunications in a national resilience and sovereignty lens. As such, government participation in or even direct ownership of cloud infrastructure, on top of the legislative to protect its citizens and national interests, can be viewed as a tool to ensure that all data, necessary to economic growth and prosperity, is protected from any actions other than what the owner carries out, and, more importantly, that no extraterritorial control can be exercised over that data. Securing the cloud requires synchronized and coordinated action from all parties in the ecosystem all in strict compliance with national regulations, and in

many cases, disregarding it leaves the door open to undesirable consequences on the national economy, or worse national security.

To secure our 'cyber borders', a suitable cloud security framework, should be either selected, or better in the case of The Organization of Islamic Cooperation (OIC), built from scratch to bring all members of the OIC ecosystem onto the same page as previously proposed in the earlier Section, that it will take an entire ecosystem to solve the cloud security problem statement holistically. However, there must be a defined boundary of the ecosystem. Thus, in the case of this paper, we shall take that as the OIC member states. A cloud security framework that not only covers governance, architecture, management standards and security, but can be developed to cover specialized economic verticals like healthcare, banking and oil and gas, to name a few, opening new channels of economic cooperation between member states.

In next section, our detailed reconsideration would be demonstrated holistically.

IV. COMPREHENSIVE RECONSIDERATION

A. *Cloud security domains*

To address the various challenges and risks of cloud services for different stakeholders in a unanimous, applicable and efficient manner, cloud security domains would present a reconsideration that is based on security by design, to senior management of user organizations to ensure a comprehensive oversight in the area of cloud security. The need for innovation and digital transformation along with adopting new business models introduces new threats and significant vulnerability and blind spots which require new ways of mitigations and countermeasures. Hosting new applications and modernizing workloads by migrating and adopting multi-cloud architecture leads to new risks such as:

1.	Potential data loss due to poorly and mis-configured or insecure interfaces and APIs
2.	Potential misuse of supercomputing power and automation tools
3.	Unauthorized access to cloud services by outsiders
4.	Limited and a lack of transparency and visibility of cloud operation.
5.	New identities and players come into business operations such as AI, Machines, Robots.
6.	Lack of talented cloud specialists across multiple technology domains

ISSN 2636-9680
eISSN 2682-9266

7.	Operation complexity and new applications development methodology
8.	New compliance requirements
9.	Lack of multiple adequate layers in defence

All of these vulnerabilities, threats, and associated risks mandate new security requirements and baselines to be in place in order to assure resilient, and sustainable business operations. A recommended list of guidelines and requirements that shall be considered are listed below:

1.	Compliance driven and adherence to local and international best practices
2.	Security and privacy by default are embedded into design
3.	Zero trust architecture for platform and related services
4.	Identity comes first; authenticate and authorize everything and everywhere
5.	Defence in depth by having a full lifecycle protection strategy through different and adequate controls at each layer
6.	Secure with visibility by integrated security operations and incident response capabilities
7.	Risk-assured continuity with no SPOF at comment level or data centre level.

Those principles and guidelines need to be embedded into the cloud security architecture to lower the risks according to the business appetite. According to the analysis above, these reconsidered domains align to prevailing international standards and incorporates regulatory and legislative requirements. These domains are classified and organized in the areas of Governance, Operational and Resilience:

Governance Considerations	Domain1 - Governance and Risk Management Domain 2 - Audit and Compliance Domain 3 - Human Resource Security Management Domain 4 - Identity and Access Management
Operational Considerations	Domain 5 - Infrastructure and Virtualisation Security Domain 6 - Data Centre Security Domain 7 - Data Security & Info Lifecycle

	Management, Encryption & Key Management Domain 8 - Change Control & Configuration Management Domain 9 - Logging and Monitoring
Resilience Considerations	Domain 10 - Security Incident Management, e-Discovery and Cloud Forensic Domain 11 - Threat & Vulnerability Management Domain 12 - Business Continuity Management Domain 13 - Interoperability and Portability

Specifically, domains in Governance Considerations would establish the mandate and policies to the Cloud Service Customer (CSC) ensuring that the use of the Cloud Service is aligned with the authorized mission and supported by the adequate personnel and resources. There is also a requirement to have a means for the management of the CSC to be assured that the use of the Cloud Service is within the approved mandate.

Domains in the Operational Considerations would list the key areas of Cloud Service Provider (CSP) operations that have direct impact on the security of the application and data hosted on the CSP cloud infrastructure such as the Data Centre, the virtualization server and the change and configuration management of the hardware, software and the application logic.

Domains in the Resilience Considerations identify capabilities that will enhance the CSP's capability to operate under duress while minimizing the security impact to the data and infrastructure. These capabilities will enable the CSP to continue operations under adverse conditions such as an ongoing security incident or disaster while actively recovering from the initial impact.

The governmental agencies and regulatory authorities are encouraged to consider and implement the roadmap in the order of Governance, Operational, and Resilience as there are dependencies that can be leveraged upon. A fully implemented set of Governance Domains will engender policies and mandates that facilitate the effectiveness of the measures described in the Operational Domains. The resulting cloud infrastructure will in turn benefit

ISSN 2636-9680
eISSN 2682-9266

from the capabilities described in the Resilience Domains such that the CSP's performance under adverse conditions can be limited.

B. *Cloud Zero Trust*

Cloud environment is a hybrid mix of technologies are fundamentally different from traditional networks and continually evolve and are subject to periodic changes, which means that the organization's approach to zero trust must be both comprehensive, agile and adaptable security strategies that ensure your organization stays ahead of emerging threats. A Zero Trust Architecture (ZTA) strategy is one where there is no implicit trust granted to systems based on their physical or network location (i.e., local area networks vs. the Internet). The Zero Trust strategy establishes a "never trust, always verify" mentality. Zero Trust requires consistent visibility, enforcement, and granular access control that can be delivered directly on the device or through the cloud to prevent unauthorized access or data loss. For the method of approaching such a strategy, following principles should be involved:

- Identify and understand all of the resources, their access points, data and application types that the organization has, as well as their storage locations, and who is accessing and using them. Based on the analysis and define your blast protect surface.
- Knowledge graph all the transaction and data flows across applications.
- Design and architect your cloud infrastructure and create microsegment boundaries between users and applications.
- Define simple and easy to understand cloud zero trust policies, controls and limits based on who should have access to what and enforce contextual access controls based on least-privilege principles. Educate users on defined cloud security policies and what's expected of them when they are accessing and using applications and data in the cloud.
- On an ongoing basis, continuously inspect - analyse and log all traffic, enforcing security policies with mitigation plans, and optimizing the policies based on the lessons to maintain the Zero Trust environment. This will ensure the identification of unusual activity and decide how to make policies more secure, allowing you to reduce the attack surface area and make changes to the architecture to further enhance your security.

In practice, to guide and approach zero trust in the cloud environment, following a baseline should be discussed:

i. Granular management of access to cloud applications and resources:

- Identity and access management for use of cloud services and for the applications and resources within those cloud services.
- Seamless Identity and access management systems covering microsegments levels of cloud services.

ii. Protect and secure cloud apps, data & infrastructure:
- Implement perimeter controls in place for all assets related to cloud services.
  Encrypt sensitive data both in rest and at transit.
- Encrypt communication channels.

iii. In-depth understanding of all resources on cloud services:
- Ensure continuous monitoring of cloud services and the apps/data located on cloud services.
- Log all data, and periodic analysis to mine any loopholes and recommend consistent workarounds to ensure zero downtime or data loss.

iv. Embrace security aspects into DevOps for cloud services:
- Include "Secure by Design" and "Data Protection by Design" principles into all applications destined to run on cloud services.
- Include security elements into DevOps processes and test security elements before and during production deployment.

v. Robust security policies, compliance and governance:
- Build a comprehensive security policy for all cloud services.
- Ensure compliance with all corporate, industry and government requirements and regulations.
- Enforce security policy through measurable security controls.

vi. Automation of security services:
- Orchestrated and automated, optimized recyclable security services to deliver best support for security standardization and consistency.

Once such a cloud zero trust is implemented, we would definitely have an in-depth understanding of data, applications, assets and risks. And we could also approach optimal, consistent, continuously enhanced and comprehensive security.

ISSN 2636-9680
eISSN 2682-9266

Besides, resilience and agility to stay ahead of evolving technologies could be assured. In the most case, it is possible to simplify and reduce operational complexities and expenditure [17].

C. *Cloud security assured in a collaborative manner*

Along with previous cloud security domains and zero trust principle, forming a cloud working group within the region including members from common cultures and interests is a necessity. Cloud security is a global requirement. However, each region has its own culture and customized requirements that must take into consideration the local business model. The main objective of the working group is to work in a collaborative manner to release cloud security framework through leveraging their knowledge and expertise in addressing cloud security requirements and data sovereignty in terms of data locality and 360-degree control and ownership.

The working group is to provide requirements for establishing, implementing, maintaining and continually improving a cloud security framework. The adoption of such framework is a strategic decision for any member of the working group. The proposed framework which is attached here addressing end-to-end security requirements considering the guidelines listed in this paper are mainly business interests, needs and objectives.

The framework considers the compliance requirements at different levels starting with the organization level, local, regional, and standard best practices. The framework considers the identity as a new perimeter and an entry point to the cloud that requires a new way of protection and security controls. Device classifications along with end point protection play a vital role in the new framework to assure data security and access control to the network domain, different segments and zones. Network according to the zero trust model shall be secured and equipped with different and multiple layers of defence, inspection, and traffic filtering ensuring a managed fault domain, availability, resiliency, and segmentation in a secure means according to business applications.

Business offerings and services that are presented in terms of applications shall be secure, and safe across the workload stack considering the adequate controls and counter measures.

Data lifecycle requires a profound governance model along with technical countermeasures considering data protection in all stages such as in motion, at rest, and in use along with data retirement as well.

One of the most important pillars of the proposed framework is the visibility of all businesses and

identifying any form of adversary and illegitimate traffic and to efficiently respond to those potential security threats.

V. DISCUSSION

A journey of thousands of miles must start from the first step. Nowadays, cloud computing security has been on the way for more than decade, while some critical steps should be down as soon as possible and as much as possible. In this paper, we have comprehensively reconsidered cloud security through security domains, zero trust and collaboration. It is recommended to apply wider cloud security domains as the implementation guidance. And it is also realized that cloud security could apply principles of zero trust and team sport to continuously improve and optimize cloud security. To sufficiently support this reconsidered cloud security approach, so that it can be implemented to support future requirements, a cloud security working group is recommended to be setup to develop a cloud security framework or cloud security as a service (in a box) to address concerns described in Section IV. In addition to the cloud service provider security standard produced by Dubai Electronic Security Centre (DESC) [31], the UAE is willing contribute our UAE Cloud Security Framework [30] towards this effort. An overview of this cloud security framework is illustrated below:

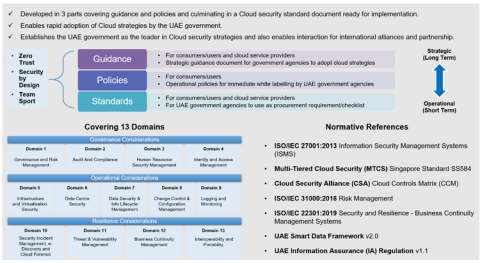

Fig. 3: Cloud security framework overview

The UAE National Cybersecurity strategy [20], one of pillars and goals of the strategy is to mobilize the whole ecosystem through local and global partnerships to jointly achieve cybersecurity goals and ambitions, which include the public and private sector, academia and international consortia. So, it would be imperative that we can establish such a working group in the OIC-CERT to solve the cloud security problem statement as presented in this paper by bringing the entire ecosystem together comprises of OIC member states, which is built by OIC member states for OIC member state. The UAE's strategy has called a PPP collaboration during GISEC 2021 which is a testimony of the recognition that we need to address cybersecurity from the perspective of team sport [33]. For another example, during GISEC 2022 [22] the UAE Cyber Security Council signed several agreements with several companies to strengthen efforts in promoting UAE's vision both locally and globally [23].

We believe this could effectively promote a whole industry approach to improve cloud security in a more reliable,

ISSN 2636-9680
eISSN 2682-9266

practical, collaborative manner. And we also willing to walk along with this journey to design and release that cloud security framework for OIC member states and lead this working group.

VI. FUTURE WORK

Cloud and 5G are two pillars of digital transformation, where cyber security is the foundation and critical business enabler. In May last year (2021), the UAE has supported the establishment of the OIC-CERT 5G Security Working Group with 12 OIC-CERT members [18]. The working group published the OIC-CERT 5G Security Framework in January this year [19] as a new approach to strengthen 5G security in the aspect of policy makers. Nowadays, much efforts have been invested for identifying and managing 5G cybersecurity risks. For example, the GSMA has conducted a comprehensive threat analysis [25] involving industry experts from across the eco-system including mobile network operators, vendors, service providers, and regulators, as well as collecting input from public sources such as 3GPP [26], and ENISA [27]. Also, some more dedicated specifications released by their working groups are also promote the 5G security, such as GSMA FS.16 Network Equipment Security Assurance Scheme-Development and Lifecycle Security Requirement v 2.0 [28], to clarify security requirements about 5G network equipment development and usage lifecycle. 3GPP TS 33.117 Catalogue of General Security Assurance Requirements [29] indicates security functions of equipment.

Similarly, referring this successful collaborative effort on 5G security, as another critical pillar of digital transformation, establishing a cloud security working group with our like-minded partners and friends to design and release the proposed cloud security framework are imperative and totally indispensable. As a result, more innovative cloud security specification, guidance and requirements for a more secure, resilient and collaborative cloud ecosystem could be efficiently released publicly. In particular, this framework would cover domains, principles and recommendations described in previous sections. Generally speaking, several next steps should be taken but not limited to:

- Continuously update cloud security risk landscape to maintain a cloud security risk register and make sure that cloud security domains are enough to address the need for OIC member states;
- Develop cloud security framework as an industry-recognized reference or specification to assist national or regional regulatory authorities in making cloud

security policies for OIC member states;
- At the same time, constantly analyse and provide insights into industry good practices, standards and security incidents to continuously improve this framework.
- Identifying like-minded partners and users within the OIC community to establish the cloud security working group.

VII. CONCLUSION

Digital transformation increasingly becomes a mandatory option for many countries and regions. And cloud and 5G not only construct the solid foundation, but also play a role of accelerator for technical innovation and well-being society. Nevertheless, with accelerating scope and severity of cloud security, and difficulties about coordination among limited resources, it has been clear that there are massive number of threats and unequal distribution. Obviously, current cloud security approach should be reconsidered. For this reason, this paper systematically present insight and consideration to approach a more secure, reliable, collaborative, diverse and vibrant cloud ecosystem nationally and regionally. Additionally, we emphasised the importance a wider cloud security domain and scope, how to use zero trust to improve cloud security, and how to assure this newly guided cloud security to be implemented in practice. Most importantly, we have argued for the urgency to establish a cloud working group and design a cloud security framework to address the problem statement in this paper based on reconsidered and analysed principles as presented. The proposed OIC-CERT cloud security framework will be a much desired and timely reference or specification for regulatory authorities to design and guide local cloud security harmoniously within OIC member states, a boon considering the rapid digital evolution that we are witnessing today. Without doubt, the cloud security working group would be an accelerator to more efficiently safeguard cloud security development to support any digital transformation plans. On the other hand, a more secure, collaborative, open, and controllable cloud ecosystem can be well constructed in the near future to safeguard the digital future for OIC member states in a period of extreme uncertainty and the non-existence of globally recognized multi-lateral norms for cloud security.

VIII. REFERENCES

[1] Mather, Tim, Subra Kumaraswamy, and Shahed Latif. Cloud security and privacy: an enterprise perspective on risks and compliance. " O'Reilly Media, Inc.", 2009.

[2] Krutz, Ronald L., and Russell

ISSN 2636-9680
eISSN 2682-9266

Dean Vines. Cloud security: A comprehensive guide to secure cloud computing. Wiley Publishing, 2010.
[3] Singh, Ashish, and Kakali Chatterjee. "Cloud security issues and challenges: A survey." Journal of Network and Computer Applications 79 (2017): 88-115.
[4] Basu, Srijita, et al. "Cloud computing security challenges & solutions-A survey." 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC). IEEE, 2018.
[5] Hayes, Brian. "Cloud computing." (2008): 9-11.
[6] Ab Rahman, Nurul Hidayah, and Kim-Kwang Raymond Choo. "A survey of information security incident handling in the cloud." computers & security 49 (2015): 45-69.
[7] Singh, Jitendra. "Cyber-attacks in cloud computing: A case study." International Journal of Electronics and Information Engineering 1.2 (2014): 78-87.
[8] Kumar, Rakesh, and Rinkaj Goyal. "On cloud security requirements, threats, vulnerabilities and countermeasures: A survey." Computer Science Review 33 (2019): 1-48.
[9] What is cloud security
[10] Cloud computing security
[11] 7 most Infamous Cloud security breaches
[12] Top 5 Cloud Security Data Breaches in Recent Years
[13] GDPR
[14] Cloud Act
[15] https://assets.extrahop.com/whitepapers/sans-survey-cloud-security-2021.pdf
[16] Secure by Design
[17] Zero Trust Architecture: NIST 800-207.
[18] OIC-CERT LAUNCHES 5G SECURITY WORKING GROUP AT GISEC 2021
[19] OIC-CERT 5G SECURITY WORKING GROUP REVEALS NEW FRAMEWORK
[20] National Cybersecurity strategy 2019,UAE
[21] Dubai Cyber security strategy
[22] https://www.gisec.ae
[23] UAE Cybersecurity Council strengthens strategy with several agreements
[24] UAE adopts largest legislative reform in its history
[25] 5G Cybersecurity Knowledge Base, https://www.gsma.com/security/5g-cybersecurity-knowledge-base/
[26] 3GPP
[27] ENISA-The European Union Agency for Cybersecurity
[28] FS.16-NESAS Development and Lifecycle Security Requirements v2.0
[29] 3GPP Specification #: 33.117
[30] UAE Cloud Security Framework, 2021
[31] Cloud Service Provider (CSP) Security Standard
[32] Middle East facing 'cyber pandemic' as Covid exposes security vulnerabilities, cyber chief says
[33] Why 2022 will usher a new decade of cybersecurity