A Survey on "Security & Privacy Overview Under Cloud Computing Adoption Framework (CCAF)"

Anulekha Goud[1], Khushboo Agarwal[2], Jaimala Jha[3]
[1, 2, 3] Dept of CSE/IT
[1, 2, 3] Madhav Institute of Technology & Science, RGPV, Gwalior, India

Abstract- *Cloud provide an advance range of services those are available from anywhere. Cloud computing is a very useful solution to many individual users and organizations. It provide enormous amount of data and program for storing and accessing over the cloud But on the other side of the coin there are various cyber security issues which might be backlash for the potentiality of services and flow of data However, there are numerous problems related to the cloud user data that essential to be addressed while using cloud computing. Among the most essential issues are: data ownership, data privacy, and storage.*

These cyber security issues have different security impact on different situation over the cloud. This paper comprises of some analysis over different security threats and provides the Review of Security under Cloud Computing Adoption Framework.

Keywords- cloud computing, characteristics of cloud computing, cloud service type, cloud computing security, framework for secure cloud, ccaf

I. INTRODUCTION

Cloud computing is a technology that enables online access to computing resources like platforms, hardware components, infrastructure, computing applications etc. without much effort. It is cost effective where service consumer will pay for what he used. Cloud computing is a technology that plays a vital role in IT industry. Not only in IT field but also smaller enterprises are adopting this technology where cloud service provider provides services and consumers access those services via a web interface. Cloud is a place where service provider keeps their resources which are available to the consumers/users and consumers are billed on pay per use basis. This technology provides its services in three layers. They are Infrastructure as a service, Software as a service and Platform as a service. These services can be deployed in three ways i.e as public cloud, private cloud and hybrid cloud. In public cloud services are made available to public over the net, in private cloud services are available only to etherize party and hybrid cloud has been used to mean two separate clouds join together (public, private, internal or external). The rise of this technology is just because of its features. Main features of cloud computing are pay-as you go, auto scaling, elasticity etc.

Firstly according to Pay-as-you go, it allows consumers to utilize services according to their need. So that one can deploy and develop applications without initial investments. Consumer has to pay according to the usage. Auto scaling feature of cloud computing technology facilitates the users to scale up or scale down the resources dynamically with respect to the requirement of their applications. The Elasticity feature allows the users to utilize the resources up to the maximum extent. Also, it provides resources to develop an application from the scratch which is a big support for growth oriented organizations [1].

II. CHARACTERISTICS OF CLOUD COMPUTING

NIST has defined cloud computing as "a model for allowing convenient, on-demand network access to a shared pool of configurable computing resources (e.g. Networks, servers, storage, applications, and services) that can be quickly provisioned and released with marginal managing effort or service provider interaction. The NIST Definition of Cloud Computing, listed in the For More Information section below [1].With cloud computing, organizations can have on-demand self-service for computing capabilities. These Capabilities are distinct for different platforms that presented over large network access. The provider's computing resources are communally assist several consumers via a multi-tenant model, with distinct physical and virtual resources vigorously assigned and reassigned rendering to consumer demand. While the place of the resources, such as storage, processing, memory, network bandwidth, and virtual machines, is not meticulous by the subscriber, it probable for the subscriber to require the country, state, or data center that supplies the cloud facilities. Cloud abilities can be delivered to the subscriber quickly and elastically, permitting the subscriber to either increase or decrease services. The capabilities available frequently appear to be indefinite to the subscriber and can be bought in any quantity at any time. Cloud systems automatically regulate and enhance resource use via a measured service capability that is appropriate for the sort of

service provided. Resource management can be observed, measured, and reported providing transparency for both the provider and the consumer of the operated service [2].

III. LITERATURE SURVEY

1. Zhang et al. (2008) explain their rationale, background, core technologies, u sage scenarios, experiments, results and their interpretations. Their method is comprehensively dedicated on the use of XML to transfer and interpret data through their security mechanism. Framework is an appropriate method provided with careful and clear explanations. This section presents the background work and overview for our proposed Cloud Computing Adoption Framework (CCAF) [6].

2. Victor Chang (2015) et.al presented a combined security method and its execution a CCAF multi-layered security was validated. The motivation and the associated literature about the CCAF security were described and it's the core technologies, which involve enterprise security concerns and resolve the EFSS security issues. Presented CCAF security with the integration of the three layered security: firewall, identity management and encryption. To determine CCAF multi-layered security as a working framework for business clouds, experiments were designed.

3. Amin Saedi (2016) et.al presented that, as an alternative, Essentialist Approach, a simplistic view of CC adoption which is based only on the technological characteristics of the revolution is prevalent. Thus, this study integrates the Technology-Organization- Environment framework as an IS adoption theory while Actor Network Theory as an Innovation Translation Approach in proposing the SMEs-CC adoption framework [8].

4. Mohammed Amoon (2016) et.al presented that, an adaptive framework to deal with the problem of fault tolerance in cloud computing environments. The framework employs both replication and check pointing methods in order to attain a reliable platform for carrying out customer requests. Also, the algorithm concludes the most suitable fault tolerance method for each selected virtual machine. Simulation experiments are carried out to evaluate the framework's performance. The outcomes of the tests show that the suggested framework enhance the performance of the cloud in terms of throughput, overheads, monetary cost and availability [9].

5. Shreya Paul (2016) et. al presented that, The huge constraint involve with sensitive data as well as its protection. So it incurs difficulty and high investment for the business group. Banking institutions and financial companies, healthcare industry, retail player and government sector strictly pursue appropriate instruction and guidelines when managing security and sensitivity of business data in cloud environment that comprise personal data, data for decision support, account related data and health related data. Tokenization based service model interchanges business organization sensitivity and confidential data with unique identification pattern is to construct for secure to embezzle the confidential and sensitive data, so that it fulfill the requirement given by the appropriate authority[10].

6. Ismail Bile Hassan (2015) et.al presented that, This study applies extended Unified Theory of Acceptance and Use of Technology (UTAUT2) along with the privacy calculus model as the base information system theories. But it is argued that UTAUT2 is a broad framework of technology adoption. For that purpose, this study integrates the UTAUT2 with privacy calculus model and enhances apparent credibility as a new variable to provision the existing UTAUT2 model. The research framework and recommendations of this study may assist to establish improved innovative e-health services as to cover the desires of the citizens through the use of health information application embedded in all in one card. Initial results to assess the validity of measurement items are presented in this paper. Further statistical analysis will be conducted in the future [12].

7. Osden Jokonya (2014) et.al presented that, This paper presented an IT adoption framework to support organizations with IT adoption governance. The authentication results from case studies recommended that the framework may be advantageous in understanding the context IT adoption problem from a holistic method. In addition the outcomes from studies recommended it probable to influence IT adoption conclusions based on manipulating the variables of the framework components.[13]

IV. CLOUD SERVICE TYPE

The second aspect well-defined by the cloud computing adoption framework. The four service types defined in the framework are layered to represent the increasing level of structure and standards. Each service type is built on, and requires the structure and standards of, the one below it. As discussed later in this paper, this progression has significant implications for both the provider and consumer of cloud services. In several cases, organizations will be pick one

or more service types, adding to the level of complexity in selecting cloud delivery methods for each and underscoring the necessity for a visual map from which to examine all characteristics of cloud delivery.

The cloud service types defined in the framework are:

A. Infrastructure cloud services(also known as infrastructure as a service, or IaaS)

These provide on-demand, pay-as-you use access to infrastructure resources, including servers, storage or network devices, that the consumer configures and controls, running the applications of their choosing. The service can be conveyed in a consumption-based business model. Infrastructure cloud services may also include an operating system with or without basic system management tools.

B. **Platform cloud services(also known as platform as a service, or PaaS)**

These services delivery compute capability (infrastructure) and a predefined middleware stack that is typically designed for creators or advanced IT users. Providers can pick out a offer with the variety of service products (stacks), configurable to varying degrees by the consumer. Examples include database, Web or application server software. Configuration and management of these middle ware resources are the responsibility of the consumer, but the provider may offer to maintain standard images once they are defined.

C. Application cloud services(also known as software as a service, or SaaS):

The service is a predefined application, such as CRM and ERP, which is typically delivered via a public cloud provider. Consumers from various groups share a distinct application instance, with virtualization technologies employed to segregate customer data and maintain privacy. Application configuration and management are the responsibility of the service provider. However, an organization may choose to implement a similar, application-based service contained by a private cloud to decrease the costs of licensing fees and other costs.

D. Business process cloud services(also known as business process as a service, or BPaaS)

The service is a predefined application, such as CRM and ERP, which is typically delivered via a public cloud provider. Consumers from various groups share a distinct application instance, with virtualization technologies employed to segregate customer data and maintain privacy. Application configuration and management are the responsibility of the service provider. However, an organization may choose to implement a similar, application-based service contained by a private cloud to decrease the costs of licensing fees and other costs.

V. CLOUD COMPUTING SECURITY

A. Trust

The concept of trust mainly consider between two parties. These parties committed in a transaction, so that ‘‘An entity A is well-thought-out to trust another entity B when entity A have faith in entity B will behave exactly as expected and required’ ’There in after, an entity can be considered trustworthy, if the parties or people involved in transactions with that entity rely on its credibility. The notion of trust in an organization could be defined as the customer’s certainty that the organization is capable of providing the required services accurately and infallibly.

B. Security Identification Of Threats

Security Identification of Threats Fundamentally securing an Information System (IS), involves recognizing exclusive threats and challenges which need to be addressed by executing the suitable countermeasures. Eventually, it recognized security requirements and particular security controls are presented to successfully integrate the security controls with the data systems functional and operational requirements, as well as other relevant system requirements (e.g. Trustworthiness, maintainability, supportability). Cloud computing due to its architectural project and characteristics executes a number of security profits, which include centralization of security, data and process segmentation, redundancy and high availability. Cloud computing has ‘‘unique characteristics that require risk assessment in areas such as availability and reliability issues, data integrity, recovery, and privacy and auditing’’

- **Confidentiality and Privacy:** Confidentiality refers to only authorized parties or systems having the ability to access protected data. The risk of data compromise growths in the cloud, due to the growth in number of parties, devices and applications involved, that indications to an increase in the number of points of access. Allotting data control to the cloud, in reverse leads to growth in the risk of data compromise, as the data turn into accessible to an improved number of parties.[19]

- **Integrity:** A key aspect of Information Security is integrity. Integrity means that assets can be changed only by authorized parties or in certified ways and refers to data, software and hardware. Data Integrity states to defending data from unauthorized deletion, alteration or fabrication. Management of an entity's access and rights to detailed enterprise resources validate that valuable data and services are not abused, embezzled or stolen. By preventing unauthorized access, organizations can achieve greater confidence in data and system integrity. Additionally, such mechanisms offer the greater visibility into determining who or what may have altered data or system information, potentially affecting their integrity (accountability). Authorization is the mechanism by which a system defines what level of access a specific genuine user should have to secure resources controlled by the system. Due to the increased number of entities and access points in a cloud environment, authorization is crucial in assuring that only authorized entities can interact with data.
- **Availability**: Availability refers to the assets of a system being accessible and usable upon demand by an authorized entity. System availability includes a systems ability to carry on operations even when some authorities misbehave. The system must have the capability to continue operations even in the probability of a security issue. Availability consider not only data and software but also hardware being available to authorized users on demand. The network in now loaded with data retrieval and processing. The cloud vendor needs to assure that data and its processing is presented to clients on their demand. System availability includes a systems capacity to carry on processes even when some authorities misbehave. The system must have the capability to continue processes even in the possibility of a security breach. Cloud computing facilities contemporary a highly confidence on the resource infrastructures and network availability at all times [4].

VI. KEY FEATURES OF CLOUD COMPUTING ADOPTION FRAMWORK

- Identifies two primary dimensions to be measured when developing a cloud computing strategy.
- Identifies key differentiated capabilities along those two dimensions.
- Identifies key capabilities and deliberations to successfully deliver and consume cloud services at the intersections defined by the differentiated points.
- Aligns abilities required with each phase of adoption.

VII. SECURITY OVERVIEW UNDER CLOUD COMPUTING ADOPTION FRAMEWORK (CCAF)

The current challenges in front of cloud community on cloud security is massive. Therefore, it essential a clear framework, which delivers an integrated approach to study cloud service performances before the implementation, the one that provisions rich execution of cloud security attributes at the implementation level, and the one that can be adopted by both cloud users and cloud providers, who propose a user-based security framework for collaborative computing systems. They explain their rationale, background, core technologies, usage scenarios, experiments, results and their interpretations. Their approach is heavily focused on the use of XML to transfer and interpret data through their security mechanism. The usage of the framework is a suitable approach provided with careful and clear explanations. These best practice techniques will keep grow as the framework has been in various applications. It is a conceptual framework like ITIL version 3 to guide organizations for the best practices. Additionally, such a framework can integrate with Cloud Computing services to provide added values for adopting organizations [16]. It is also an architecture framework focused on the delivery of a security service, in the form of developing a multilayered security for data centers.

VIII. FRAMEWORK FOR SECURE CLOUD

Figure 2 below shows our framework for secure cloud computing. It involves of three essential security mechanisms each one of them comprises significant challenges associated to cloud security and privacy. These properties are:

A. Security and privacy requirements:

This mechanism use to recognize security and privacy requirements for the cloud such as authentication, authorization, integrity, etc. Security concerns confidentiality, availability and integrity of data or information. It includes Authentication, Authorization and Access control (AAA).

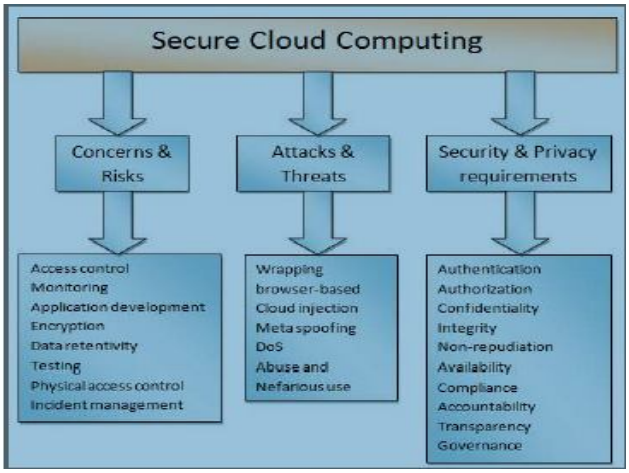

Fig.2 framework for secue cloud

On the other hand, privacy concerns the adherence to various legal and non-legal norms. It includes agreement, persistence restriction and legitimacy which all guarantee that a cloud deployment meets the requirements imposed by law. The International Standards Organization (ISO), suggested a number of information security requirements, they are:

- **Identification and Authentication management:** User identification and authentication problem in the cloud environment results from its multitenancy feature which allows adversary of malicious users to utilize the cloud. To alleviate this problem, CSPs are essential to employ approaches that help discretely verify and authorize cloud users when they logon to their accounts. Authentication and user identification are usually accomplished by employing usernames and passwords when using web browser to access the cloud. Authorization and access control: in a cloud environment, especially public cloud, many users at different locations in the world access the cloud with different privileges. Users are granted privileges by CSPs based on their account type.

- **Authorization and access control:** In a cloud environment, especially public cloud, many users at different locations in the world access the cloud with different privileges. Users are granted privileges by CSPs based on their account type. The challenge here is how to control access priorities, permissions and resource ownerships of authenticated users on the cloud. Also, one of the most difficult problems is how to monitor and control the activities of those privileged users.

- **Confidentiality:** Due to a large number of users and access points to the cloud, data is vulnerable to unauthorized access by unauthorized users. Confidentiality ensures that information is available only to those authorized to have access. Confidentiality becomes vital in public clouds due to its accessible nature. Data confidentiality could be exposed on the cloud due to multitenancy, user authentication and software applications.

- **Integrity:** Integrity states to protecting cloud data and Program from unauthorized deletion, modification, theft or fabrication, this guarantees that data has not been tampered with or abused. Integrity includes data accuracy, completeness and ensures Atomicity, Consistency, Isolation and Durability (ACID). These properties should be robustly imposed across all cloud computing model.

- **Non-repudiation**: This property use to ensures that the sender of a message cannot deny the message was sent and that the recipient cannot deny the message was received. This can be achieved using techniques such as digital signatures, timestamps and confirmation receipt services

- **Availability:** This property refers to cloud data, software and also hardware being available, usable and accessible to authorized users upon demand. CSPs should be able to continue providing customers with services even in case of the existence of security breaches, malicious activities or system faults.

- **Transparency:** The operation of the cloud should be sufficiently clear to users and CSPs. Users must be able to get a clear overview of where and how their data will be handled. They also must be able to determine who the cloud provider is and where his responsibility ends. Governance: data on the cloud is vulnerable since it is processed and stored remotely. Customers have concerns about why their personal information is requested and who will use it. There are also threats associated with virtualization and resource sharing. Policies and procedures should be applied to protect the cloud from attacks, threats and data loss.

B. Attacks and threats:

Warns from different types of attacks and threats to which clouds are vulnerable. Before defining types of attacks in clouds, we must identify the attackers themselves and their impact on the security of cloud systems. Cloud attackers may be categorized as follows:

- **Random:** the most common type of attackers uses simple techniques to randomly scan the internet in order to find

susceptible computers. They deploy well known tools that should be easily detected.

- **Weak:** These are semi-skilled attackers who target specific cloud providers by modifying data and made data publicly available.
- **Strong:** They are organized, skilled and well financed groups of attackers who target particular applications and users of the cloud. Generally, they form criminal groups specialized in large scale attacks.
- **Substantial:** They are motivated, highly skilled attackers who can't be easily detected either by the organizations they attack or by the law enforcement and investigative organizations specializing in e-Crime or cyber security.

C. Concerns and risks:

Concerns and risk usually pay attention to risks and concerns about cloud computing. We discuss each guideline in detail in the following sub-sections.

- **Access control:** how can cloud users manage access control threats and risks when the levels and types of access control used by cloud providers are unknown?
- **Monitoring**: how can accurate, timely and effective monitoring of security and privacy levels achieved in business-critical infrastructure when its providers are not prepared to share such information at SLA?
- **Applications development:** how to accomplish application improvement and preservation in the cloud when CSPs are responsible to?
- **Encryption:** how can the cloud user manage encryption and assign responsibilities across the borders between the cloud service providers and organization?
- **Data retentively:** how can the cloud user attain appropriate assurance that the data have been actually and securely removed from the system by the cloud provider and are not just made inaccessible to him?
- **Testing:** how can consumers test the effectiveness of security control when these tests may not be made available by CSPs?
- **Physical access control**: how can the cloud user attain requirements for physical access when its measures are established and fully controlled by CSPs?
- **Incident management:** how can the cloud user determine appropriate [5].

IX. CONCLUSION

Cloud computing is a new standard of computing utility that assure to provide more elasticity, enhance computing capabilities and less expense IT services to end user over cloud. This paper present basic introduction of cloud computing along with cloud services model and study various cyber security challenge present over cloud also provide concluded impact of cyber security issues on cloud computing security.

REFERENCES

[1] M. Vijayalakshmi, D. Yakobu, D. Veeraiah, N. Gnaneswara Rao, “Automatic Healing of Services in Cloud Computing Environment”, ISBN No.978-1-4673-9545-8

[2] Shirley Radack, “Cloud Computing: A Review Of Features, Benefits, And Risks, And Recommendations For Secure, Efficient Implementations”, Itl Bulletin For June 2012

[3] ibm.com/legal/copytrade.shtml/ibm.com/ibm/cloud/resources.html#5

[4] Dimitrios Zissis ∗ , Dimitrios Lekkas, “Addressing cloud computing security issues”, Accepted 13 December 2010

[5] Ahmed E. Youssef1 and Manal Alageel, “A Framework for Secure Cloud Computing”, ISSN (Online): 1694-0814IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 3, July 2012

[6] Victor Chang, Muthu Ramachandran, “Towards achieving Data Security with the Cloud Computing Adoption Framework”, 1939-1374 (c) 2015 IEEE.

[7] Victor Chang, Yen-Hung Kuo, Muthu Ramachandran, “Cloud Computing Adoption Framework a security framework for business clouds”, S0167-739X(15)00311-8/27 September 2015.

[8] Amin Saedi, “Cloud Computing Adoption Framework: Innovation Translation Approach”, 978-1-5090-2549-7/16/©2016 IEEE.

[9] Mohammed Amoon, “Adaptive Framework for Reliable Cloud Computing Environment”,DOI 10.1109/ACCESS.2016.2623633, IEEE 2016

[10] Shreya Paul, Atma Prakash Singh, Shafeeq Ahmad, “Tokenization Based Service Model for Cloud Computing Environment”,10.1109@INVENTIVE.2016.78300

[11] Victor Andres Ayma Quirita, Gilson Alexandre Ostwald Pedro da Costa, “A New Cloud Computing Architecture for the Classification of Remote Sensing Data”, 1939-1404 © 2016 IEEE

[12] Ismail Bile Hassan , Masrah Azrifah Azmi Murad, Rozi Nor Haizan Binti Nor, Salfarina Binti Abdullah, “Towards Developing A New I-P Technology Adoption Framework : A Research Road Map”, 978-1-4799-8822-8/15 © 2015 IEEE.

Osden Jokonya, Jan H. Kroeze, John A. van der Pol, "A FRAMEWORK TO ASSIST ORGANIZATIONS WITH IT ADOPTION GOVERNANCE", 978-1-4799-4093-6/14©2014IEEE.