Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 03, March -2018

Intertwined Security and Privacy Controls Using SaaS in Cloud Computing

Reenu Sindhu, Dr. Aman Jain

[1]Research Scholar, Singhania University, Jhunjhunu, Rajasthan.

[2]Professor, Deptt. of Computer Science
Maharishi Arvind Institute of Science and Management, Jaipur

Abstract— *Cloud computing (CC) picked up a far reaching acknowledgment as a worldview of computing. The fundamental point of CC is to diminish the requirement for customers' interest in new hardware or software by offering adaptable cloud services, with a client receiving the rewards of the compensation per utilize approach. CC requests tending to numerous security and protection issues: the two issues (vulnerabilities, dangers, and attacks) and arrangements (controls). The proposition examines every one of these classes of issues and arrangements, classifying them as either security-related issues, protection related issues, or entwined security and security issues. The principle commitments of the proposal are twofold: to start with, utilizing the above order of the issues; and second, the writing audit of the security and protection issues in CC inside the categorization structure. The significant lessons picked up amid this exploration incorporate confirmation of the decisive part that security and privacy solutions play and will keep on playing in receiving CC by customers; understanding various vulnerabilities, dangers, and attacks; and identifying controls for these issues. Moreover, the sheer number of references to trust (in the two issues and arrangements), showed a noteworthy part of trust in CC.*

Keywords—*CC, Security, SaaS, IaaS, PaaS etc.*

I. INTRODUCTION

Cloud computing is a model for empowering helpful, on- demand network access to a common pool of configurable processing resources (e.g., frameworks, servers, accumulating, applications and associations) that can be instantly provisioned and discharged with unimportant organization exertion or administration center association. This cloud show progresses accessibility and is made out of five crucial characteristics, three delivery models and four deployment models." [1]

Cloud is an registering model that insinuates both the applications decided as administrations over the Internet, the equipment and framework software in the datacenters that give those services. Cloud Computing is treated as the high potential paradigm used for deployment of applications on Internet. This concept also explains the applications that are broaden to be accessible through the Internet. Cloud applications use large data centers and effective servers that host web applications and services. Cloud Computing is rapidly being accepted as a universal access appliance on the Internet.

Cloud computing is different from the traditional concept of the cloud and by the very nature in which it is distributed. When a user develops a web application in the cloud computing environment IDE, there might be five different instances of the application running in five distinctive data centers all through the world. Additionally, this application could be pulling data from divided capacity in three distinct data centers all through the world. There may be eight different instances of the "engine" running in eight different data centers, all working and processing the information that the user’s application is taking in and fanning out.

II. CLOUD DELIVERY MODELS

As indicated by NIST, the cloud model is made out of three service models:

- **Software as a Service (SaaS):** This model enables the customer to get to an application trough a client interface, usually a web browser, the consumer has few if no control over the cloud environment. The cloud service provider is in charge of the total framework including the applications, databases, and so forth. The consumer does not supervise or control the concealed cloud establishment including network, servers, operating frameworks, storage, or even individual application limits, with the conceivable exemption of restricted client particular application configuration settings [2]. With the SaaS delivery model, CC consumers are given the capability to use the CC provider’s applications running on the cloud infrastructure (in contrast to PaaS, where they run their own applications). In SaaS, the cloud users do not have control or authority to manage the underlying cloud infrastructure or even the individual applications [3]. There are possibilities of that user will have limited access to configuring settings in related to applications. SaaS services include email and office productivity applications, customer relations management, enterprise resources planning, social networking, data management, etc. [4].

- **Platform as a Service (PaaS):** This show enables the shopper to get to a sending domain without the cost and multifaceted nature of owning the underlying hardware and software, it is a popular model used by developers. In addition to the infrastructure, the underlying software is provided such as operating system, application server, database management system, etc [5]. PaaS is able to integrate all kinds of current business, typically as application server, business capability access, business engine, and business open platform. To downwards, it calculates infrastructure capability according to business requirement, and calls hardware resources based on the API provided by IaaS. it delivers business dispatch service, monitoring every kind of resources in real time and passing those resources to SaaS end users via API.

- **Infrastructure as a Service (IaaS):** This model allows the consumer to have a high level of control and responsibility for the cloud environment, the cloud service provider provides the virtualized hardware such as data storage, server hardware, network infrastructure and the like. The operating system and others configurations remain the responsibility of the consumer. The ability gave to the consumer is to provision processing, storage, networks, and other central processing assets where the shopper can send and run subjective software, which can incorporate working frameworks and applications[5]. Usually, there are three ways to apply IaaS: public cloud, private cloud and hybrid cloud that have been mentioned before. Amazon EC2 utilizes public server pools in infrastructure. More private services will use a set of public or private server pools in a company's datacenter. If the datacenter environment of the company is used to make software development, in this way, the public, private and hybrid cloud are all available. Besides, the cost of EC2 used as temporary extensive resources is quite low and shortens the development or testing cycle.

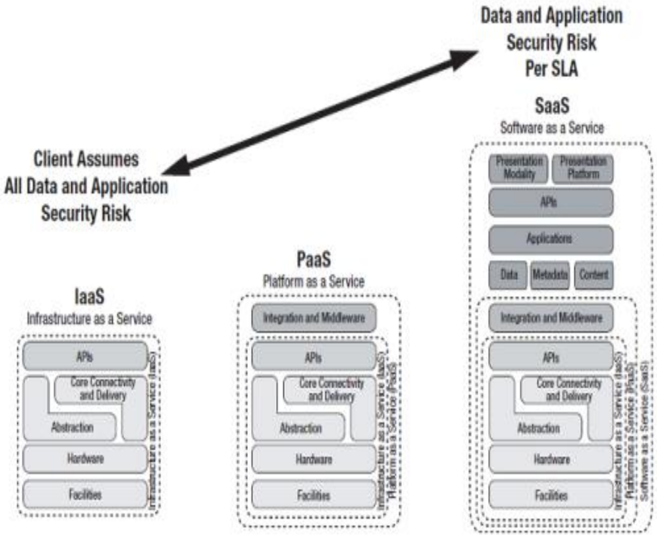

Fig. 1: Cloud delivery models

III. CLOUD DEPLOYMENT MODELS

The cloud deployment models move by ownership, size, and access, there are four customary cloud deployment models:

- **Public Cloud:** A public cloud delivers its service for public use. The whole system is usually shared by various organizations. Any customer with a credit card can pay to rent cloud services under the "pay-as-you-go" pricing model. The customers do not have direct control over the cloud system. A public cloud is usually run by a commercial cloud provider .This model is the most popular deployment model because it is, by definition, accessible to the public. E.g., Google Drive, Dropbox are public clouds. The resources are shared among the clients, it is considered as the riskiest solution due to the ignorance of with whom the resources are shared [6]. NIST gives the accompanying meaning of public cloud "The cloud framework is provisioned for open use by the overall population[7].

The advantages of a public cloud include:

1) **Low Cost:** The nature of the public cloud is that you only pay for what you use. So as an organization grows or shrinks so do the associated costs. By comparison a private cloud might require an infrastructure designed to cope with growth (thus more expensive); likewise no costs saved if the needs shrinks. Other significant savings are related to costs associated with the size and work of the in-house IT team.

2) **Increased Efficiency:** As public clouds have devoted groups dealing with keeping up the framework, downtime is more averse to be an issue. On top of this if applications are hosted by CC provider, updates are usually managed by the provider, saving upgrading expenses.

The disadvantages of a public cloud include:

1) **Wrong Provider:** There are genuine perils of picking a wrong public cloud provider. If a provider does not keep hardware up to date, users may suffer compliance and execution speed issues.
2) **Reduced Control:** As the public cloud is controlled by a CC provider, users do not have as much control as in a private cloud.
3) **Perceived Weaker Security:** Security may be a drawback to an public cloud, be that as it may, as is demonstrated by the abnormal state of public cloud appropriation by a portion of the world's greatest organizations the security concerns are not valid if the public cloud is hosted by a CC provider aware of security issues, and their impact on customers' perception [8].

- **Private Cloud:** This model is dedicated to a single consumer, the company can manage the cloud environment itself or use a cloud service provider, it provides a higher control of the protection and confidentiality [6]. The cloud infrastructure is provisioned for a single organization. This organization normally has dynamic or flighty computing needs, or requires coordinate control over the calculation condition. Generally the private cloud system is installed behind firewalls under the control of its organization, so it only permits access by authorized customers from this organization. Note that a private cloud can be configured internally by the organization itself, or externally by a third-party cloud provider. It might be owned, managed, and worked by the association, an outsider, or some mix of them, and it might exist on or off premises." [7].

The advantages of private clouds include the following ones:

1) **Security:** The security is within the organization's control. In spite of the fact that while numerous rush to acknowledge private clouds as being more secure [9], the huge range of various sending writes and levels of security inside private facilitating situations puts forth this a to a great degree bold statement [9]. The truth for me is that a private cloud is similarly as vulnerable to security risks as an public cloud. The main contrast is that an public cloud might be more appealing to invade than a private cloud as there is a more extensive measure of data in it .
2) **Performance:** If a private cloud is sent inside an association's firewall it expands the execution contrasted with utilizing general public cloud off premise.
3) **Control and Flexibility:** Organizations have more control in private clouds and as a result deploying new applications and make changes can be done in quick manner.

Table 1: The deployment models of Cloud Computing

Type	Description	Reference
Public Cloud	The cloud service policy, value and costing are defined by a service provide and used by general public.	The NIST Definition of Cloud Computing (Mell and Grance 2011)
Community Cloud	The cloud infrastructure is shared by several organizations belonging to a single group or community. The infrastructure is hosted by third party of by the community.	
Private Cloud	The cloud model for a single organization and is maintained by organization or third parties	
Hybrid Cloud	The cloud infrastructure is a combination of two or more cloud models (private, community or public)	

IV. CLOUD COMPUTING SECURITY

Reviews of senior-level IT managers show [10], security is reliably one of the main five worries, alongside, particularly, the security identified with the accessible innovation existing apart from everything else. Security concerns emerge on the grounds that both the customer data and program dwell inside the suppliers premises. In almost every study done about cloud computing the essential reason accommodated not receiving is security concerns [11].

Putting business-basic data in the hands of an outer supplier still petrifies of generally managers. Only by relinquishing some control over the data will companies then capture the cost economies that are available after joining the cloud computing technology. A company must determine when the trade-off is worthwhile. In choosing the exchange off a portion of the inquiries to consider are:

- What happens if the data put away or handled on a cloud machine moves toward becoming bargained?
- Will the customer be informed of that?
- If the customer does not know, how will they notify their constituents, especially when data breach notification laws are in place?
- How will the customer know to improve their security?

The truth of the matter is that holding the data in the cloud is not really any less secure than leaving it on internal servers connected to the Internet. The current case in the UK [11], about a programmer who hacked his way into the US Government organize demonstrates that apparently secure systems are similarly prone to be broken. Organizations should be sensible about the level of security they may accomplish within their own business, and how that may contrast with a cloud provider. It is well known that more than 70% of intellectual property breaches are a result of attacks made from within the organization. Despite this, security will be raised as a concern regarding cloud computing for many years to come. There is still much work to be done before more formalized standards are set in place. In the same way that some banks have hesitated longer than others in offering Internet banking facilities so shall it be with cloud computing. Some organizations may evaluate the risks and may adopt cloud computing quickly, while other more conservative organizations may bemore apt to observe from the "sidelines" and watch the development sun fold [10]. In addition, a recent study by IDC [12], shows that about 88.5% of the customers that are likely to avoid using cloud computing cite security as the main reason for this denial (see Figure 2).

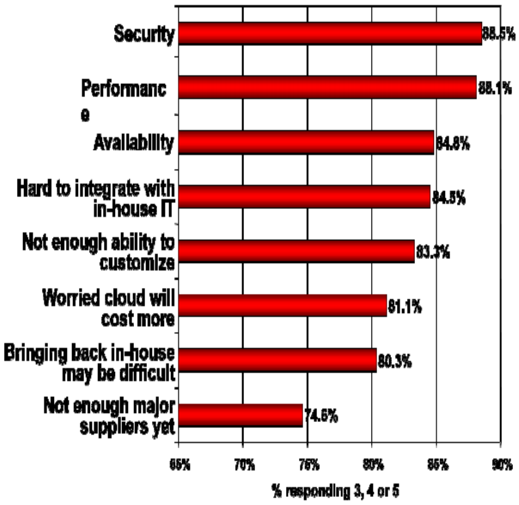

Fig. 2: Shows that about 88.5% of the customers that are likely to avoid using cloud computing cite security as the main reason for this denial

V. SECURITY REQUIREMENTS

Security is needed at the different levels that include:

- Server access security.
- Internet access security.
- Database access security.
- Data privacy security.
- Program access security.

Applying security protocols includes both the "software side" security and the "hardware side" security. A good cloud computing provider must have secure enough policies in place to keep the data safe from the dangers and vulnerabilities stated in the previous section. Some of the important security requirements are:

- **Confidentiality:** Ensuring that information is not disclosed to any unauthorized parties.
- **Integrity:** Ensuring that information held in a system, is a proper representation of the information intended and that it has not been modified by an unauthorized person
- **Availability:** Ensuring that data preparing resources are not influenced inaccessible by malicious action.
- **Non-repudiation:** Ensuring that assentions made electronically might be demonstrated to have truly happened.
- **Physical security:** On the "hardware side" of security there are several well defined protocols in the industry, such as the professional security staff utilizing video surveillance, cutting edge IDS, and other electronic means for guarding a datacenter. Moreover, when a worker never again has a honest to goodness business reason for getting to the datacenter, that representative's benefits for getting to the datacenter ought to be promptly denied, Physical security protocols should be applied to all datacenters and backup centers and wherever user data is stored or used.

VI. MAIN SECURITY ISSUES IN CLOUD COMPUTING

Security is becoming more and more challenging cloud computing due to its popularization nowadays. When we enjoy the convenience that cloud computing brought to us, meanwhile, the risks are also approaching with it. In the recent two years, massive security issues happened frequently with cloud computing providers. On 15 March 2009, Microsoft Azure was suspended around 22 hours, however the detail of cause has not been given by Microsoft. On 11 June 2009, Amazon EC2 benefit was hindered for a few hours because of the broken electrical equipment that provided datacenter harmed by lightning stoke (Wu et al., 2011).

- Privacy management

One of the feature of cloud computing is the participation of huge number of users, and it is inevitable to have privacy problems. Many users worry that their private data will be collected by cloud technology. Therefore, plenty of service providers promised to avoid collecting user's privacy information and keep them confidential if they acquired that information. Nevertheless, users still cannot be satisfied with the guarantee is credible, while their concerns make sense. In cloud computing environment, one of the most important is that user data is not stored in local device, instead, it is stored in the cloud, in which some sensitive data will result in privacy leakage. Despite numerous cloud guidelines about not uploading sensitive data to cloud, it is not a perfect solution and probably neutralize certain benefits brought by cloud. In addition, it hinders the development of cloud computing. Besides, the on demand service provided by cloud calculates service fees by accessing user data on the cloud, and some local laws or commercial operation have particular requests concerning the storage and utilization of data. In this situation, an effective mechanism is required to monitor and audit data without leaking sensitive content.

Most of privacy management in cloud computing emphasizes the use of cloud server by applying management component in the cloud. With the assistance of service provider, users are able to control their own sensitive information. By using obfuscation, even without the help of service provider or malicious action of service provider, users still can secure their privacy data. Another privacy manager offers encryption to privacy data and transfers it to the cloud through privacy manager. This mechanism is based on a shared key by user and a privacy manager that proceed obfuscation and de-obfuscation to conceal the real content in cloud but display authentic result in client side. Moreover, the privacy manager completely utilizes TPM to protect obfuscation key, strengthening privacy protection feature.

The above mentioned privacy managers are all used obfuscation technology. Generally, obfuscation means that user creates a function f(x) in terms of x which indicates privacy data and upload f(x) to server. In the meantime, the service provider calculates f'(x) with acquired f(x) but without knowing of x in a certain cloud service. Then, the service provider will send f'(x) as the result of service to the user for further processing. Though obfuscation is an excellent method, there are still some mistakes in calculation due to unware of input data. In addition, it will increase the calculation obstacle on user's information processing with frequent computation.

For cloud stored data, on the one hand, users wish for a service provider that can give correct result according to their inquiries, on the other hand, they do not want service provider to know the actual content, namely, implementing encrypted data query. Therefore, a keyword search with protected privacy feature that uses PEKS has been created. In the scenario where B sends email to A, by utilizing the trapdoor provided by A, the third-party tests if certain word exits in the email without aware of the content. This scheme allows for a service provider partially participating in content decryption and search but is not able to read whole plain text, which helps with releasing pressure on user information processing with protected privacy.

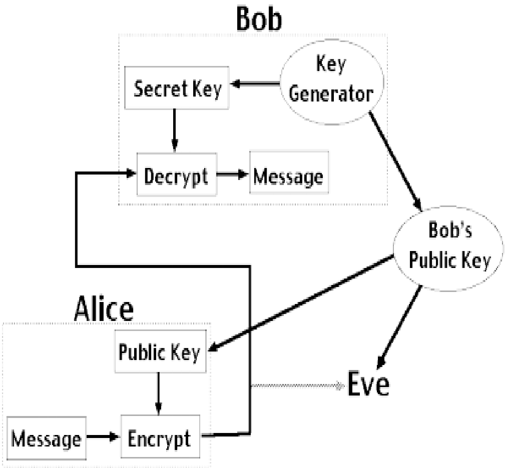

Fig. 3: Public Key encryption

- **Data security and confidentiality**

In cloud computing, users cannot have full controllability of their data when they upload them to cloud, Compared to traditional computing, it brings new challenges. In terms of cloud computing model, IaaS usually provided by the interface of web service which means accessed by web browser. PaaS is achieved by applying the combination of above mentioned technologies, while XML is the carrier of protocols belongs to network application layer in data transmission and parameters and there is evidence indicating that certain security problems related to web service and browser have a connection with it such as attack to XML signature. In addition, the security problem of browser not only should be solved by transmission layer security technology, but also enforces XML encryption in the core code of browser.

Due to the security issue with browser, the identification based on it is also vulnerable. Besides, the feature on integrity and virtual machine applied to cloud, there are existing malwares, metadata fraud and DoS attacks to server. Thus, in the view of application, it is supposed to focus on web browser and web service framework to enhance security. According to the web 2.0 application, a system file framework aiming at securing file storage service was published. By utilizing the result of secured client cross domain scheme, an independent file system service was created for web service that users regain the control of data. Another mechanism was given, which separates the content and format of document meanwhile it encrypts them before transmission going to outside. It lowers the risk of content leakage also containing an optimized document authorization access method.

VII. Intertwined Security and Privacy Controls for Cloud Computing

There are various measures and controls which are taken to secure the cloud in terms of security and privacy and to prevent from various issues. They are shown in Fig. 16 and discussed here.

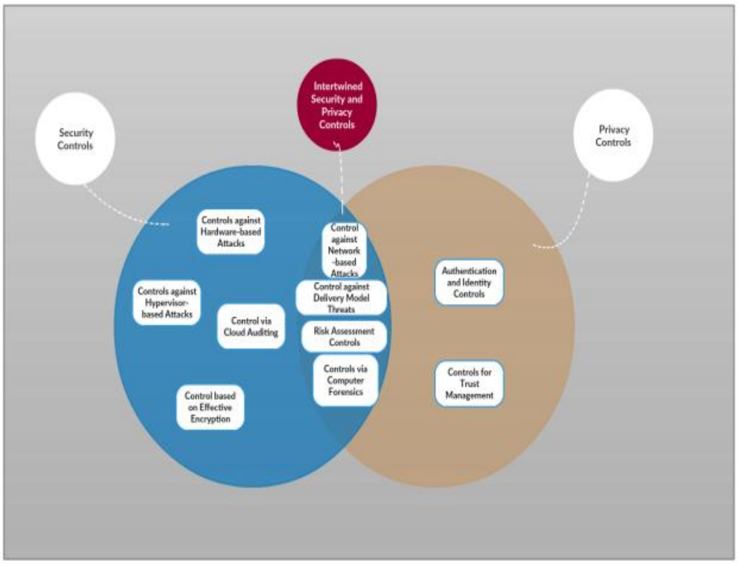
Intertwined Security and Privacy Controls
Security Controls
Privacy Controls
Controls against Hardware-based Attacks
Control against Network -based Attacks
Controls against Hypervisor-based Attacks
Control against Delivery Model Threats
Authentication and Identity Controls
Control via Cloud Auditing
Risk Assessment Controls
Controls via Computer Forensics
Controls for Trust Management
Control based on Effective Encryption

Fig.4: Security only, Privacy-only, and Interwined security and privacy controls in CC

***Controls Against Network-based Attacks*:**
In order to enable secure connection of between one virtual machine to another, providers need to protect the traffic inside their cloud infrastructure and the traffic coming from the outside. Coppolino et al .outline procedures, for example, firewalls, intrusion detection systems, anti-virus gateway, monitoring incoming and active movements that are usually utilized by associations and providers. They argue that the countermeasures should ensure system availability, data confidentiality and data integrity at channel and system's application level. To ensure system availability, cloud providers must defend their cloud environment before, during and after the DOS and DDOS attacks. Defense can be inherent to the system design (always on), or might require activation, which is preceded by DOS attack detection [13].

Controls against Delivery Model Threats
There are various intertwined security and privacy problems affecting cloud delivery models (IaaS, PaaS, and SaaS). Controls for these problems require, among others, strong end-to-end encryption, and a trust management scheme. Each delivery model (IaaS, PaaS, and SaaS) requires authorization in a public cloud to prohibit unauthorized accesses. Integrity is also an essential requirement—for checking data correctness. The high availability and integrity of the services requires strong security mechanisms in the underlying network

VIII. LITERATURE SURVEY

Ronald L. Krutz and Russel Dean Vines et al. [14] in this paper, "Cloud Security - a Comprehensive Guide to Secure Cloud Computing"aims to provide insight into the capabilities, vulnerabilities, advantages and trade-offs of the cloud while also describing methods of gaining the benefits of the cloud computing with minimal risk. The book clarifies issues and concerns about privacy and security that may arise when being introduced to cloud computing, such as geographical dispersion, size and structure. Guidelines on how to maneuver the field of cloud computing are provided in an extensive way.

Tim Mather, SubraKumaraswamy and Shahed Latif et al. [15] in this paper, tries through a systematic investigation of what constitutes cloud computing, what it offers in terms of security and answer what is wrong with security in cloud computing. Implications of cloud computing security on protection, inspecting and consistence on both the cloud specialist co-op and the client are likewise investigated in the book. Different perspectives on security for larger organizations versus small to medium-size business are included in the book as well.

D. Zissis et al. [16], in this paper, the authors list different security threats depending on the service model delivered. Axis today serves corporate customers with their hosted cloud service which can be described as a SaaS. For this type of service, the authors claim that security threats such as interception, modification of data at rest and in transit and session hijacking are most likely. These are specific vectors that we have taken into consideration when making the proposal and model. Moreover, they recommend executing a trusted third party (TTP) that can encourage secure cooperation's between two parties. The Axis TTP service takes the role of TTP in the Axis-hosted cloud service, whose role is to serve certificates and point devices 4 Introduction to the correct cloud. Thus, parallels can be drawn between the authors' suggested optimal solution and Axis' current solution.

Zhidong Shen; Qiang Tong et al. [17] In this paper, have examined "The security of cloud computing framework empowered by put trusted in computing technology ". Cloud computing gives individuals the best approach to share conveyed resources and administrations that have a place with various associations or sites. Since cloud computing share distributed resources through the network in the open condition, in this way it makes security issues essential for us to build up the cloud computing application. In their paper, they focus on the security prerequisites in cloud computing condition. They proposed a technique to fabricate a trusted processing condition for cloud computing framework by coordinating the confided in registering stage into cloud computing framework. They propose a model framework in which cloud computing framework is joined with confided in registering stage with put stock in stage module. In their model, some essential security services, including verification, confidentiality and integrity, are given in cloud computing framework.

Sabahi, F. et al. [18] in this paper, has clarified in his paper about "Cloud computing security dangers and reactions". IT associations have communicates worry about basic issues, (for example, security) that exist with the across the board execution of cloud computing. These sorts of concerns start from the way that data is put away remotely from the client's area; indeed, it can be put away at any area [18].

IX. RESEARCH METHODOLOGY

Research methodology is a process of managing and solving research problems systematically. To achieve the goals of research we can use different methods and techniques. For addressing the research questions and objectives, the exploratory approach is used. An exploratory study is a method for increasing new bits of knowledge and clarifications for particular issues.

Systematic Literature Review (SLR): Systematic Literature Review (SLR) is characterized as recognizing, assessing and interpreting the accessible significant work for a specific theme or phenomenon of interest. The researchers should put a significant amount of work and effort to identify published research results related to his research work. SLR is used mainly to summarize the existing state of the art, and to determine the gaps in it.

Privacy is a crucial issue in cloud computing because a customer's information and business logic must be entrusted to cloud servers owned and maintained not by the customer but by cloud providers. Although there are so many security-only and privacy-only problems, there are also occurrences where security and privacy are intertwined. The hijacking was facilitated by the two-factor authentication setup allowed by the Google account recovery process which denied the victim his administrative privileges. Such account security issue was addressed by removing the two-factor recovery system. Private and sensitive data are vulnerable to hacking by malicious attackers especially in public clouds. Furthermore, when individuals and corporate cloud users put their data in the hands of their cloud providers, it remains unclear who has the authority to own and maintain custody of such information.

The key thing about SAML is that it enables Internet SSO. SAML Eliminates the need to maintain multiple authentication credentials such as passwords in multiple locations. It is important for three reasons:

1. It increases the security by eliminating additional credentials which eliminates opportunities for identity theft.
2. It eliminates phishing opportunities by eliminating the number of times a user needs to log in over the Internet using one of those username login forms and in fact recently a major SaaS application was subjected to phishing attack.
3. It increases application access by eliminating barriers to usage so user no longer have to type in a password to basically click on a link there in the application.
4. It eliminates administration time and costs by eliminating those duplicate credentials and also by eliminating all those extra help desk calls to reset those lost passwords.

We introduce categorization of security and privacy issues into *security-only* issues, *privacy only* issues, and *intertwined security and privacy* issues. This separation of issues has proven useful, resulting in a better organization of this survey. Next, we divide security and privacy *issues* into problems and solutions. In turn, *problems* include *vulnerabilities, threats and attacks (VTAs)*. The main contributions of the thesis are twofold: first, using the above categorization of the issues (security-only, privacy-only, and intertwined); and second, the literature review of the security and privacy problems and solutions within this categorization framework.

We have significantly deepened our understanding of numerous security and privacy problems (vulnerabilities, threats, and attacks), which we studied after categorizing them as security-only problems, privacy-only problems, and intertwined privacy and security problems. We identified and studied many new controls for these problems, analogously categorized as security-only controls, privacy-only controls, and intertwined privacy and security controls. In addition, the sheer number of references to trust (in both problems and solutions), demonstrated a significant role of trust in CC, and a need for more security and privacy solutions based on trust in an explicit way. We believe now that—based on the advancement of cloud computing and increasing number of cloud users—the body of knowledge on security, privacy *and trust* in cloud computing will continue to grow fast.

CONCLUSION

Cloud computing is rising as a major and beneficial technology of present day and future. CC gives the advantage of quick deployment, cost efficiency, large storage space and simple access to the framework whenever and anywhere. In this Paper, we talk about the significant parts of security and protection in CC. We present arrangement of security and privacy issues into security-just issues, privacy only issues, and interweaved security and privacy issues. This division of issues has demonstrated helpful, bringing about a superior association of this overview. Next, we isolate security and protection issues into issues and arrangements. Thusly, issues incorporate vulnerabilities, dangers and attacks (VTAs). The primary commitments of the theory are twofold: to begin with, utilizing the above arrangement of the issues (security- only, privacy only, and entwined); and second, the writing audit of the security and security issues and arrangements inside this order structure.

REFERENCES

[1] Shun-Ren Yang and Yi-Bing Lin, ”Modeling UMTS Discontinuous Reception Mechanism”, IEEE Transactions on Wireless Communications, vol. 4, no. 1, January 2005.

[2] Peter Mell. (2011) 'The NIST Definition of Cloud ', Reports on Computer Systems Technology, sept., p. 7.

[3] S. Subashini and V. Kavitha, “A survey on security issues in service delivery models of cloud computing,” J. Netw.Comput. Appl., vol. 34(1), Jan.2011, pp. 1–11.

[4] Z. Gilani, A. Salam, and S. UlHaq, "Deploying and managing a cloud infrastructure : real world skills for the CompTIA cloud+ certification and beyond," Wiley, Jan. 2015.

[5] P. Mell, T. Grance, The NIST Definition of Cloud Computing (2011), http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf, accessed on 2017-01-10.

[6] E. Thomas, M. Zaigham, and P. Ricardo, Cloud Computing: Concepts, Technology & Architecture, 1st ed. Prentice Hall/PearsonPTR, 2013.

[7] M. Peter and G. Timothy, The NIST Definition of Cloud Computing, U.S. Department of Commerce Std. 800-145, 09 2011.

[8] S.Y. Zhu, R. Hill, and M. Trovati, "Guide to security assurance for cloud computing," Springer, 2015.

[9] T.W. Shinder, Y. Diogenes, and D.L. Shinder, "Windows Server 2012 security from end to edge and beyond: architecting, designing, planning, and deploying Windows Server 2012 security solution," Elsevier, 2013.

[10] McKendrick J., (2011), “Loud Divide: Senior Executives Want Cloud, Security and IT Managers are Nervous”, [Accessed 04-20-2011]: http://www.zdnet.com/blog/serviceoriented/cloud-divide-senior-executives-want-cloud-security-and-it-managers-are-nervous/6484

[11] Kynetix Technology group, (2009), “Cloud Computing Strategy Guide”, [Accessed 12-02- 2010]: https://sites.google.com/site/cloudmanual/success-factors

[12] IDC data survey source, (2008), IDC Enterprise Panel, survey number=244

[13] A.Y. Sarhan and L.T. Lilien, “An Approach to Identity Management in Clouds without TrustedThird Parties,” Trans of the 11th Western Michigan IT Forum, vol. 1(1), Kalamazoo, Michigan, Nov. 2014, pp. 18-27.

[14] R. L. Krutz, R. D. Vines, Cloud security: A Comprehensive Guide to Secure Cloud Computing (2010)

[15] T.Mather, S.Kumaraswamy, S.Latif, Cloud Security and Privacy, http:// www.di.fc.ul.pt/~nuno/PAPERS/security3.pdf, accessed on 2017-03-09.

[16] D. Zissis, D. Lekkas Addressing cloud computing security issues (2010), http://www.cs.joensuu.fi/~parkkine/LuK2015/ CloudCompSecurity-FutureGenerCompSyst2012.pdf, accessed on 2016-12- 13.

[17] W. Li and L. Ping, "Trust model to enhance security and interoperability of cloud environment," Cloud Computing, pp. 69-79, 2009.

[18] F. Rocha, S. Abreu, and M. Correia, “The Final Frontier: Confidentiality and Privacy in the Cloud,” IEEE Computer, vol. 44 (9), Sept. 2011, pp. 44–50.