Security and Privacy Problems in Cloud Computing

Richa kunal Sharma[#1], Dr. Nalini Kant Joshi[#2]

Research Scholar, Career Point University, Kota, Computer Science
Asso.Prof. Deptt. of Computer science and Engineering
Rajasthan Technical University Kota

Abstract

Cloud computing has formed the conceptual and infrastructural basis for tomorrow's computing. The global computing infrastructure is rapidly moving towards cloud-based architecture. While it is important to take advantages of could base computing by means of deploying it in diversified sectors, the security aspects in a cloud-based computing environment remains at the core of interest. Cloud based services and service providers are being evolved which has resulted in a new business trend based on cloud technology. With the introduction of numerous cloud-based services and geographically dispersed cloud service providers, sensitive information of different entities is normally stored in remote servers and locations with the possibilities of being exposed to unwanted parties in situations where the cloud servers storing that information are compromised. If security is not robust and consistent, the flexibility and advantages that cloud computing has to offer will have little credibility. This paper presents on the cloud computing concepts as well as the all these classes of problems, categorizing them as either security-related issues, privacy-related issues inherent within the context of cloud computing and cloud infrastructure.

Keywords - *Cloud computing, cloud service, cloud security, cloud privacy, distributed computing, security.*

I. INTRODUCTION

Cloud computing is a technique to store and access data or a program through internet instead of computer hard drive. Cloud is a metaphor for the Internet [1]. Cloud provides efficient computing by centralizing data reposition, processing and information measures. A simple example of Cloud computing is E-mailing. The Cloud look after the Email management software and server which is totally managed by the Cloud service provider e.g. Yahoo, Google etc. on virtual machines, which brought out of a new transition known as virtualization[1]. Cloud computing is the virtualization of the computer programs through an internet connection rather than installing application/s on every computer. Due to the wide use of virtualization in implementing Cloud infrastructure brings security concerns for the Cloud services. There are various important security issues, which are considered while using virtualization for Cloud computing. Security concerns such as undetected network attacks, allocating and de-allocating resources and Virtual Machine (VM) hypervisor have been seen. Like-wise virtualization, there are a number of various Cloud aspects associated with Cloud computing. Cloud issues can be grouped into various dimensions such as Cloud security including privacy, compliance, and legal issues.

Security processes that were once visible are now concealed behind levels of abstraction. This lack of visibility creates a number of Cloud Security issues. The focus is to identify issues in Cloud computing, which considers vulnerabilities, threats, attacks and their countermeasures to provide security at each layer of Cloud computing. These issues along with others have been looked intoand various countermeasures havebeen provided but Cloud needs to be more secure and robust to fulfil the daily needs of the clients. There is a need for development of a process that would help to analyse all high/medium/low risks and provide countermeasures for the same.

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 [2,3].

Since cloud computing involves multi-tenancy and sharing of information, there are higher risks of violation of privacy and confidentiality. When users put their data into a public cloud, they no longer have control over confidentiality of these data. This demonstrates that cloud computing is not ideal for confidentiality considering that some organizations prefer to develop their own services and keep their data private.

As workloads are migrated to shared infrastructures, users' private information face elevated risk of unauthorized access and exposure. Organizations have expressed their discomfort to store their data and applications on systems residing outside their on-premises data centres [4]. This may expose sensitive individual and corporate information, affecting both legal and regulatory requirements of the data being stored or transported [6]. also, privacy-protection organizations voice their doubts. For instance, the World Privacy Forum executive director expressed concerns about the transfer of large city records to a CC service provider [5].

Security and Privacy Definitions. Security can be defined as follows [9]: "Security is the right not to have one's activities adversely affected via tampering with one's objects."

In an equally succinct way, we can define privacy as follows [9]: "Privacy is the right to have information about oneself left alone." Similarly, Rocha et al. [7] define privacy as the selective control of access of "self." Selective control refers to the process where individuals control their interaction and information exchange with others. To assure their privacy, individuals try to control their openness to others. Pearson [8] explains that the level of openness between individuals is determined by their relationship and the value given to the information safeguarded. Privacy can be generally described as the dynamic process whereby individuals regulate the degree of their openness to others.

A. Cloud Computing Deployment Model

Cloud computing architecture has three main deployment models which are defined below:

Private Cloud: This infrastructure exists on a private network and is managed by the organization in its internal enterprise data centre or by the cloud provider and may reside on premises or off-premises. It is more secure because only the organization who owns it has access to operate and control over service delivery environments. It aims to address concerns on data security and offers greater control and does not provide benefits like reducing capital and operational costs.

b) Public Cloud This infrastructure is designed for wide-ranging groups or public, owned and managed by a cloud provider. The resources are dynamically provided ondemand on pay-per-use approach. It is subjected to malicious attacks which is why it is not much secure. It provides various benefits to its consumers like scalability, location independence, flexibility and no initial capital investment on infrastructure.

Hybrid Cloud This infrastructure is a combination of clouds that are linked to one another by standardized technology to share data and applications regardless of ownership and location. It offers more flexibility and greater control over the application by bringing together the advantages of each other while addressing the limitations as well [10]

Community Cloud This cloud infrastructure is designed to be used by multiple organizations in a single community that has common interests. Everyone in the community cloud has free access to data and applications. Many other cloud deployment models are being developed because of different needs of different consumers. One such example is a Virtual PrivateCloud– a way ofutilizing public cloud infrastructure in a private manner and inter-connecting the resources through virtual private network (VPN), is an example of such models [11]. Fig. 1 gives a brief overview of cloud computing deployment models with their attributes.

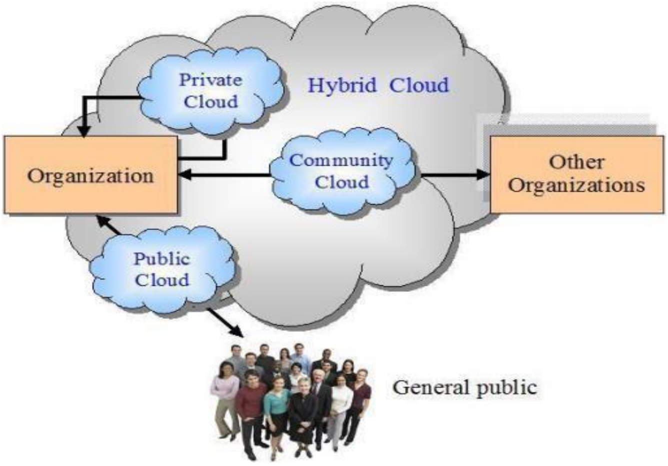

Figure 1. cloud computing deployment models.

B. CLOUD COMPUTING SERVICE DELIVERY MODELS

There are three elementary cloud service delivery models which are denoted as SPI MODEL. The term SPI is an acronym that stands for Software, Platform and Infrastructure [12].

a) Software as a Service (SaaS) In the Software as a Service (SaaS) model, the client can access the provider's infrastructure through an interface. Most commonly used interfaces are web browsers. In this model a single instance on the service provider's end supports multiple access instants on the client's side. One main advantage of this model is that the consumer does not incur software licensing cost [13]. However, on the service end, licensing costs are greatly reduced since only a single instance of an application is required to support multiple clients' access. In this model, customers do not have the privileges to manage the cloud infrastructure. Besides providing efficiency, the model raises concerns since the customers cannot view how data are flowing and stored in the cloud. The security tasks are left to the service provider to ensure the security and privacy of client data considering that they serve multiple clients. The most common security concerns with this delivery model are data security. Clients' data are stored outside their premises under the protection of third-party service providers, therefore, raising concerns. Service providers ensure this through a complex scheme of data encryption such that they cannot gain access to the data themselves. However, malicious criminals can decrypt the complex encryption to gain access or destroy the stored data. Network security poses another security risk since the data flow occurs over the network vulnerabilities that can be easily exploited leading to a data breach. Security as the client retrieves and stores the data needs to be ensured. Hackers take advantage of such vulnerabilities to attack [14]

b) Platform as a Service (PaaS) In the platform as a service (PaaS), a development platform is offered as a service. The platform enables clients to build their applications that run on the service provider's infrastructure [13]. The platform supports programming languages such as Python, Net and Java among other support tools that enable the clients to create custom applications. Although the customer has no control over the fundamental infrastructure like storage and other hardware, they have control over the kind of end user application deployed to them. The ability of the clients to develop an application on the platform means that they share some security responsibilities. Therefore, there are two parties involved, the service provider and the client. This raises more security concerns as the vulnerabilities increase with the use of the web applications [14].

c) Infrastructure as a Service model (IaaS) For the Infrastructure as a service model (IaaS), the service provider provides basic computing abilities to the clients. The client gains control of the storage, networks, and other computing capabilities by renting the services from the provider. Though the customer has control over the storage system and operating system, they do not control the overall cloud infrastructure. Understanding how the three models relate is essential [12]. IaaS forms the foundation of all the models with PaaS following onto which SaaS builds itself on. Fig 2 below indicates how the delivery models relate and the subscriber as well as service provider functions in the different models. IaaS offers the client with more security controls. The vulnerability in this model occurs in the virtualization techniques. Virtualization security is, therefore, essential while working with IaaS [14].

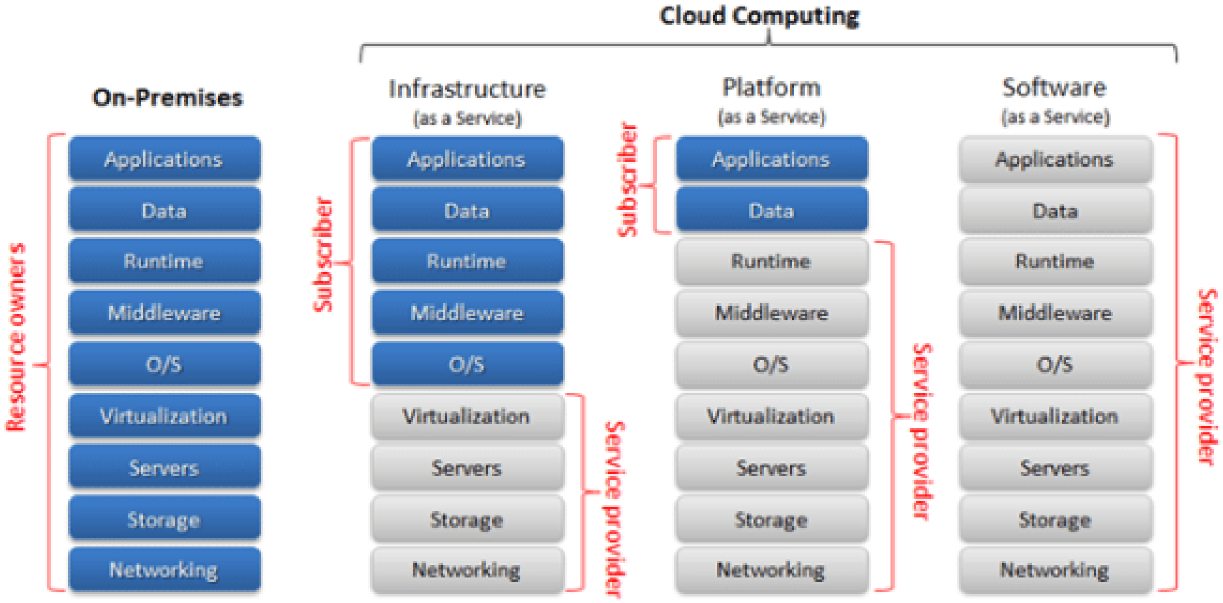

Figure 2: Cloud computing delivery models

II. A SURVEY OF THE RELATED RESEARCH

Researchers are continuously working in the area with many fronts. This section highlights the already accomplished research contributions available in the literature, which is given as follows:

Ahmed EL-Yahyaoui& Mohamed DafirEch-Chrif EL Kettani present a new fully homomorphic encryption scheme from integers. Our encryption scheme can be used essentially to secure sensible data in cloud computing. The proposed scheme uses a large integer ring as cleartext space and one key for encryption and decryption, i.e. it is a symmetric encryption scheme.[15]

Yunchuan Sun,1 Junsheng Zhang,2 Yongping Xiong,3 and Guangyu Zhu4 present a new work of Data security and privacy protection issues are relevant to both hardware and software in the cloud architecture. This study is to review different security techniques and challenges from both software and hardware aspects for protecting data in the cloud and aims at enhancing the data security and privacy protection for the trustworthy cloud environment. In this paper, we make a comparative research analysis of the existing research work regarding the data security and privacy protection techniques used in the cloud computing.[16]

Vaishali Singh & S. K. Pandey present a paper is to provide the recent advancements and a broad overview of the existing literature covering various dimensions of the Cloud security. The paper also includes various directions for future research in Cloud security based on the related published work and industry trends. This may be very useful, particularly for the entry level researchers, who wish to conduct the research in these related areas.[17]

Monjur Ahmed and Mohammad Ashraf Hossain presents a review on the cloud computing concepts as well as security issues inherent within the context of cloud computing and cloud infrastructure. If security is not robust and consistent, the flexibility and advantages that cloud computing has to offer will have little credibility.[18]

Naseer Amara, Huang Zhiqui&Awaais Ali present a paper highlights cloud computing architectural principles, cloud computing key security requirements, cloud computing security threats and cloud computing security attacks with their mitigation techniques, and future research challenges.[19]

Ramakrishnan Krishnan Present a paper on all these classes of problems and solutions, categorizing them as either security-related issues, privacy-related issues, or intertwined security and privacy issues. The main contributions of the thesis are twofold: first, using the above categorization of the issues; and second, the literature review of the security and privacy issues in Cloud Computing within the categorization framework. The major lessons learned during this research include confirmation of the decisive role that security and privacy solutions play and will continue to play in adopting Cloud Computing by customers; understanding numerous vulnerabilities, threats, and attacks; and identifying controls for these problems. In addition, the sheer number of references to trust (in both problems and solutions), demonstrated a significant role of trust in Cloud Computing.[20]

III. SECURITY PROBLEMS IN CLOUD COMPUTING

Clouds can be flexible and cost-efficient. In a cloud infrastructure, sensitive information for a customer is kept on geographically dispersed cloud platforms, under direct control of the cloud —not of the customer. Securing users data in a cloud is one of the most challenging tasks Cloud resources (such as software, platforms, and infrastructure) are vulnerable to abuse, theft, unlawful distribution, harm, or compromise. Among others, there is a risk that user's information can be leaked to a competitor. Unauthorized access to data stored in clouds can be minimized through ensuring security.

Cloud Computing Security**:** A security model is needed in cloud computing to coordinate scalability and multi-tenancy with requirement for trust [22]. Since cloud computing involves pooling of resources so that multiple users can have access to them, data stored or managed in a cloud are likely to face security issues. When organizations move to cloud environment with their identities, information and infrastructure, they must be willing to give up some level of control. The organization must trust its CC systems and providers, but still be able to verify cloud processes and events [21, 24].

The fundamentals of trust and verification are access control, data security, compliance and event management. CC services and mechanisms include: authentication, authorization, data encryption, data privacy, and multi-tenancy.

CC services and mechanisms include: authentication, authorization, data encryption, data privacy, and multi-tenancy.

Table 1 shows relationships between cloud security requirements and cloud services and mechanisms. These requirements are mandatory to achieve integrity and coherence in cloud systems.

Cloud Security Requirements	Cloud Service/Mechanism				
	Authentication	Authorization	Data Encryption	Data Privacy	Multi-Tenancy
API's	No	No	No	Yes	Yes
Cloud Software	Yes	No	Yes	No	Yes
Data Protection	No	No	No	Yes	Yes
Hardware Virtualization	No	No	No	Yes	Yes
Software Virtualization	No	Yes	No	No	Yes
Utility Computing	No	Yes	No	No	Yes
Virtualization	No	Yes	No	No	Yes
Web Portals	No	No	No	Yes	Yes

Table 1. Cloud Security Requirements vs. Cloud Services/Mechanisms [52].

Categories of CC security include: identity, information, infrastructure, network, and software security [23].

***A. Problems: Vulnerabilities, Threats and Attacks*:** Cloud computing presents various risks to an organization that have adopted it. Cloud security issues are determined greatly by the cloud service delivery model and deployment model. High security levels can be more easily achieved in private clouds than in public clouds [25]. Other top security problems in cloud computing include insecure interfaces and APIs, malicious insiders, shared technology issues, account or service hijacking, and unknown risk profiles. The following subsections discuss some of the security problems (VTAs) in cloud computing; they are also shown in Fig.3.

***B. a) Buffer Overflow Attacks*:** A buffer overflow is the condition when the data sent to the buffer is beyond its capacity [26]. When a program runs, the system allocates a section of the adjacent area of memory to store various types of data; this memory space is called a buffer. With a lack of validation of data written into a buffer, buffer overflow can occur: an excess data overflows the buffer and overwrites the adjacent memory. The data that overflows to adjacent memory makes the system more vulnerable to subsequent attacks since it allows attackers to deploy more sophisticated programs that cause bigger damage. Successfully exploited buffer overflow vulnerability can modify the value of a variable in memory, or even hijack the process, execute malicious code, ultimately leading to a full control of the host [27]. The simplest and most common form of the buffer overflow attack combines an injection technique with an activation record corruption. The attacker locates an "overflowable" variable, then feeds the program a large string that simultaneously overflows the buffer (in order to change the activation record) and contains the injected attack code [28]. Attackers use code specifically designed to cause buffer overflows [29]. Buffer overflow is among the worst bug attacks on a cloud since it is difficult to detect and fix. Early detection and intervention are recommended to ensure that a minimal or no damage is caused by a buffer overflow [30].

***b) Cloud Authentication Attacks*:** Research studies reveal that any authentication mechanism related to web applications and cloud should provide high security, easy to use interface and support user mobility. The customers prefer to access their applications from different locations and different devices such as desktop, laptop, PDA, smart phones, cell phones etc. Those needs pose significant requirements to the security of applications. The broad range of user requirements introduces wide range of attack vectors in the cloud that makes the security of cloud applications a thought-provoking matter. Cloud service providers need to ensure that only legitimate user is accessing their service, and this points out to the requirement of a strong user authentication mechanism. But there exist numerous attacks that can create loop holes in the authentication mechanism and hence identifying the most secure authentication mechanism with high user acceptability is a big challenge in the cloud environment. Thus, an in-depth idea of attacks on authenticity and corresponding prevention techniques are required to draft a fool proof authentication mechanism for cloud environment. Figure3 gives a pictorial representation of the attacks on authenticity and in the sections that follows, a detailed description of the attacks and the possible solutions are given.

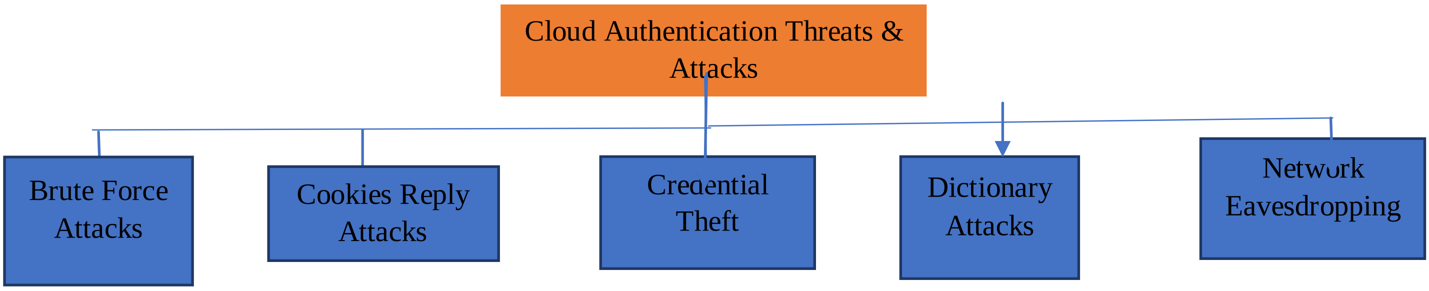

Fig.3Cloud Authentication Threats and Attacks

*c) **Cloud Malware Injection Attacks***: In Cloud Malware Injection Attack an attacker tries to inject malicious service or virtual machine into the cloud. In this type of attack attacker creates its own malicious service implementation module (SaaS or PaaS) or virtual machine instance (IaaS), and try to add it to the Cloud system. Then, the attacker has to behave so as to make it a valid service to the Cloud system that it is some new service implementation instance among the valid instances. If the attacker succeeds in this, the Cloud automatically redirects the requests of valid user to the malicious service implementation, and the attacker code starts to execute. The main scenario behind the Cloud Malware Injection attack is that an attacker transfers a malicious service instance into cloud so that it can achieve access to the service requests of the victim's service.

*d) **DOS Attacks and Mobile Terminal Security***: DOS attacks and mobile terminal security level attacks are quite common.

DOS Attacks: Denial-of-Service (DOS) and distributed denial of service (DDOS) are among the major security threats in cloud computing [34]. A DOS attacks occur when an intruder attempts to deny authorized users access to information and cloud services [31]. A DDOS attack involves the use of multiple corrupted systems to target and corrupt a certain cloud in order to induce DOS attacks [32,33].

DDoS attacks on an application layer can take advantage of inefficiencies in a web application. They are often difficult or impossible to detect at the network layer, so many upstream protection measures may be unable to help, forcing a website operator to rely on a combination of cloud-based or proxy-based solutions, as well as best practices in application design and management of its supporting architecture (including HTTPD, MySQL server, etc.).

This requires making the right choices when deciding which software to use, its configuration, and the design of one's own software. For instance, an application which makes resource intensive calls to a MySQL server is easily attacked by DOS creating relatively low volumes of transactions intended to stall the SQL server from operating normally. This is an example of a case when an attacker can identify a flaw or inefficiency in a web application and use for a DOS attack that is not easily detected at the network layer [35].

DOS and DDOS attacks can be addressed through an efficient DDOS detection and prevention technique based on a Third Party Auditor (TPA) [31].

Mobile Terminal Security and DOS: These problems originated with cell phone users. Waseem et al. [36] identified that these users are usually uninformed about security and confidentiality matters. The authors believe that mobile phone customers often fail to use their devices appropriately, exposing themselves to crackers (malicious hackers). Attackers may use such lax security to mount DOS attacks preventing users from accessing their cloud services. Meanwhile, the user's CC provider will be striving to deal with the attack using substantial CC resources, further increasing probability that the cloud services continue being unavailable to customers. Eventually, the crackers can simply erase, manipulate, or misplace private information stored by cloud users [36].

e) Insecure API's:Cloud Computing providers expose a set of software interfaces or APIs that customers use to manage and interact with cloud services. Provisioning, management, orchestration, and monitoring are all performed using these interfaces. The security and availability of general cloud services is dependent upon the security of these basic APIs. From authentication and access control to encryption and activity monitoring, these interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy. Furthermore, organizations and third parties often build upon these interfaces to offer value-added services to their customers. This introduces the complexity of the new layered API; it also increases risk, as organizations may be required to relinquish their credentials to third parties in order to enable their agency.

f) Malicious Insiders**:** A malicious insider is an employee of the Cloud Service Provider who abuses his or her position for information gain or for other nefarious purposes e.g. a disgruntled employee. The threat of a malicious insider is well-known to most organizations. This threat is amplified for consumers of cloud services by the convergence of IT services and customers under a single management domain, combined with a general lack of transparency into provider process and procedure. To complicate matters, there's usually very little or no visibility into the hiring standards and practices for cloud employees. This kind of situation clearly creates an attractive opportunity for an adversary - ranging from an amateur hacker, to organized crime, to corporate espionage, or even nation state sponsored intrusion. The extent of access granted could enable such an adversary to reap confidential data or gain complete control over the cloud services with little or no risk of detection.

The impact that malicious insiders can have on an organization is substantial, given their level of access and ability to infiltrate organizations and assets. Brand damage, monetary impact, and productivity losses are just some of the ways a malicious insider can affect an operation. As organizations adopt cloud services, the human element takes on an even more profound importance. It is critical therefore that the consumers of cloud services understand what providers are doing to detect and defend against the malicious insider threat. [37]

g) SQL Injection Attacks: Structural Query Language (SQL) is a language used to program and manage data in relational databases. Originating in 1986, SQL has gained so much popularity due to its practicality and ease of use that these days most databases are formed around an implementation of SQL, for instance, MySQL or Microsoft SQL Server. Databases can hold sales data, customer information, medical records and financial information, meaning their contents could have enormous value. Therefore, they have been heavily targeted by malicious parties since the early days of computing.

Apart from the regular vulnerabilities that could be exploited to gain access to the system holding the database, there is another method of attack which could be utilized to gain access to the contained information or even to eradicate the data; SQL Injection.

SQL Injection attacks target the database directly by attempting to interact with it via for instance a web form field or a URL. The goal there is to send commands to the server which will then return an entire table containing usernames and passwords or even credit cards. This is how many of the massive breaches (up to 100+ million users) over the last decades have occurred.

IV. PRIVACY PROBLEMS IN CLOUD COMPUTING

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 [39, 38].

Cloud Computing Privacy:Since cloud computing involves multi-tenancy and sharing of information, there are higher risks of violation of privacy and confidentiality.

When users put their data into a public cloud, they no longer have control over confidentiality of these data. This demonstrates that cloud computing is not ideal for confidentiality considering that some organizations prefer to develop their own services and keep their data private.

As workloads are migrated to shared infrastructures, users' private information face elevated risk of unauthorized access and exposure. Organizations have expressed their discomfort to store

their data and applications on systems residing outside their on-premises data centres [40].

This may expose sensitive individual and corporate information, affecting both legal and regulatory requirements of the data being stored or transported [42]. also, privacy-protection organizations voice their doubts. For instance, the World Privacy Forum executive director expressed concerns about the transfer of large city records to a CC service provider [41].

A. Problems: Vulnerabilities, Threats and Attacks:Privacy is certainly one of the issues where the personal information is exploited, and the following are some of the vulnerabilities, threats and attacks.

***B. a) Broken Authentication and Compromised Credentials*:** Broken authentication refers to the situation where there is an inadequate mechanism for validation of user certificates (as a special case, a certificate could assure a user' identity). Breach of privacy for various users of cloud services may result when the providers cannot confirm that access to data in the cloud is performed by legitimate users [44,43].

Authentication and access control are effective only in uncompromised computing systems. Ineffectiveness or absence of security controls in CC environments is among the causes of compromised credentials [45]. It is the role of providers to ensure that there is an efficient authentication system to ascertain authenticity of customers' credentials.

b). Data Breaches:A data breach is a confirmed incident in which sensitive, confidential or otherwise protected data has been accessed and/or disclosed in an unauthorized fashion. Data breaches may involve personal health information (PHI), personally identifiable information (PII), trade secrets or intellectual property.

Common data breach exposures include personal information, such as credit card numbers, Social Security numbers and healthcare histories, as well as corporate information, such as customer lists, manufacturing processes and software source code. If anyone who is not specifically authorized to do so views such data, the organization charged with protecting that information is said to have suffered a data breach. If a data breach results in identity theft and/or a violation of government or industry compliance mandates, the offending organization may face fines or other civil litigation.

c) Data Location Problems:Cloud Computing offers a high degree of data mobility. Consumers do not always know the location of their data. In most cases, this does not matter. For example, emails and photographs uploaded to Facebook can reside anywhere in the world and Facebook members are generally not concerned. However, when an enterprise has some sensitive data that is kept on a storage device in the Cloud, they may want to know the location of it. They may also wish to specify a preferred location (e.g. data to be kept in the UK). This, then, requires a contractual agreement, between the Cloud provider and the consumer that data should stay in a particular location or reside on a given known server. The issue is that consumers are, sometimes, not aware of the implication of this and thus no such contract is agreed beforehand. Although, cloud providers should take responsibility to ensure the security of systems (including data) and provide robust authentication to safeguard customers' information, under the circumstance, what is required is that the providers not just inform the consumers, as a matter of course, but also provide the necessary information that the consumer may not be aware of. An example is the UK laws with respect to data privacy. It is required by law that the personal data of UK citizens must reside within the country. The Cloud provider must know this and advise consumers accordingly. If the consumers know this then obviously, they can suggest, even demand, that the data be kept on a device that physically resides within the UK. Many other countries have legal requirements with respect to the location and movement of personal data.

d) Problems Related to Data Ownership and Content Disclosure: Another crucial privacy matter emerging from cloud computing is the problem of data ownership. As users put their data on a cloud service, the privacy of the data could be lost.

Besides, the users are at risk of losing ownership authority over their data as well as the right of disclosure by push away ownership to the cloud service providers [49]. Despite the lawful ownership, along with the right of disclosure being at the disposal of the original data owner [46], owner's right might be violated. For instance, some cloud providers, as data custodians, retain the right of disclosure, while others do not.

When a CC service provider contractually becomes the data owners as well as the data custodian, a privacy issue emerges. Even with outmoded IT services, the best practice is to separate duties, in which a different entity owns the data while another remains the chief custodian of that data [47]. Even so, with cloud computing, that paradigm has shifted, making the service provider the owner and custodian of all information stored or transmitted through their cloud. Such practices violate the core principles of duties separation and job rotation, which are crucial doctrines in best practices for data security [48].

e) Virtualization Problems: Virtualization was introduced to facilitate sharing of huge expensive resources among different application environments. This enables an organization to interact with their IT resources in a more efficient way and allows for a much greater utilization. Virtualization technologies rapidly became a standard technology used in IT organizations [50].

Virtualization of resources is achieved with the help of a hypervisor, which allows a dynamic allocation of resources to virtual machines (VMs). Cryptography is used in virtual systems of a cloud to secure data in transit from private premises to the cloud, but data must be decrypted in memory. This creates a loophole through which privacy breaches may occur since virtualization enhances almost transparently the memory pages of an instance, enabling obtaining if data by a malicious provider.

CONCLUSIONS

Research studies reveal that Cloud environment needs to recognize the importance of security and privacy within its various areas. There should be a bond of trust and privacy between the service provider and the client. Security must be viewed as a continuous process to meet the changing needs of a highly volatile computing environment. There is a need to have a holistic approach regarding cloud computing security methodology, which can be used in general, in any service model, at any stage till the client is using the service. There should be self-awareness from the client side too, regarding its own security and privacy alsoin this Thesis, we discuss the major aspects of security and privacy in Cloud Computing. This separation of issues has proven useful, resulting in a better organization of this survey. Next, we divide security and privacy issues into problems. In turn, problems include vulnerabilities, threats and attacks (VTAs).

REFERENCES

[1] S. K. Pandey (2013).“Cloud Computing: A new era of Information Technology Management”. The Chartered Accountant Student (Students’ Journal). Vol. SJ 4 Issue 1. pp. 10-12.

[2] C. Wang, Q. Wang, K. Ren, and W. Lou, “Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing,” IEEE INFOCOM, 2010, pp. 1–9.

[3] P.L.S. Kumari and A. Damodaram, “An Alternative Methodology for Authentication and Confidentiality Based on Zero Knowledge Protocols Using Diffie-Hellman Key Exchange,” Intl. Conf. on Information Technology, 2014, pp. 368–373.

[4] B. Grobauer, T. Walloschek, and E. Stocker, “Understanding Cloud Computing Vulnerabilities,” IEEE Secur. Priv. Mag., vol. 9 (2), Mar. 2011, pp. 50–57.

[5] G.-J. Ahn, M. Ko, and M. Shehab, “Privacy-Enhanced User-Centric Identity Management,” IEEE Intl. Conf. on Communications, 2009, pp. 1–5.

[6] A. Behl, “Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation,” World Congress on Information and Communication Technologies, 2011, pp.

[7] 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.

[8] S. Pearson, “Taking account of privacy when designing cloud computing services,” ICSE W. on Software Engineering Challenges of Cloud Computing, 2009, pp. 44–52.

[9] J. Ramey and P.G. Rao, “The systematic literature review as a research genre,” IEEE Intl. Professional Comm. Conf., 2011, pp. 1–7.

[10] N. T. T. G. M. Bones, "Cloud Computing Security Issues and Challenges," International Journal of Computer Networks (IJCN), vol. 3, no. 5, 2011.

[11] D. S. L. G. J. e. a. Fernandes, "Security Issues in Cloud environments: a survey," International Journal of Information Security, vol. 13, p. 113, 2014.

[12] K. Hashizume, D. Rosado, E. Fernández-Medina and E. Fernandez, "An analysis of security issues for cloud computing", J Internet ServAppl, vol. 4, no. 1, p. 5, 2013.

[13] " Cloud computing service and deployment models: layers and management", Choice Reviews Online, vol. 50, no. 07, pp. 50-3896-50-3896, 2013.

[14] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, vol. 34, no. 1, pp. 1-11, 2011.

[15] Ahmed EL-Yahyaoui& Mohamed DafirEch-Chrif EL Kettani“Data Privacy in Cloud Computing” 2018 4th International Conference on Computer and Technology Applications.

[16] Yunchuan Sun,1 Junsheng Zhang,2 Yongping Xiong,3 and Guangyu Zhu4” Data Security and Privacy in Cloud Computing” International Journal of Distributed Sensor Networks Volume 2014, Article ID 190903, 9 pages.

[17] Vaishali Singh & S. K. Pandey” Research In Cloud Security: Problems And Prospects” International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR) ISSN 2249-6831 Vol. 3, Issue 3, Aug 2013, 305-314.

[18] Monjur Ahmed1 and Mohammad Ashraf Hossain2” Cloud Computing And Security Issues In The Cloud” International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014.

[19] Naseer Amara, Huang Zhiqui&Awaais Ali “Cloud Computing Security Threats and Attacks with their Mitigation Techniques” 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery.

[20] Ramakrishnan Krishnan “Security and Privacy in Cloud Computing” Western Michigan University,2017.

[21] M. Waseem, A. Lakhan, and I.A. Jamali, “Data Security of Mobile Cloud Computing on Cloud server,” Open Access Libr. J., 2016, vol. 3.

[22] W.R. Claycomb and A. Nicoll, “Insider Threats to Cloud Computing: Directions for New Research Challenges,” IEEE 36th Annual Computer Software and Applications Conf., 2012, pp. 387–394.

[23] D. Daniels, “Identity Management Practices and Concerns in Enterprise Cloud Infrastructures,” J Gate Acad. J. Database, vol. II, no. 14, 2013, pp. 2321–5518.

[24] S. Hajra et al., “DRECON: DPA Resistant Encryption by Construction,” Springer, 2014, pp. 420–439.

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

[26] D. Naccache et al., “Buffer Overflow Attacks,” Encyclopedia of Cryptography and Security, Boston, MA: Springer US, 2011, pp. 174–177.

[27] D. Fu and F. Shi, “Buffer Overflow Exploit and Defensive Techniques,” 4th Intl. Conf. on Multimedia Information Networking and Security, 2012, pp. 87–90.

[28] C. Cowan, P. Wagle, C. Pu, S. Beattie, and J. Walpole, “Buffer overflows: attacks and defenses for the vulnerability of the decade,” Foundations of Intrusion Tolerant Systems, 2003, pp. 227–237.

[29] C. Cowan et al., “StackGuard: Automatic Adaptive Detection and Prevention of Buffer-Overflow Attacks, ” 7th USENIX Security Symp., San Antonio, Texas, Jan. 1998.

[30] K.S. Kumar and N.R. Kisore, “Protection against Buffer Overflow Attacks through Runtime Memory Layout Randomization,” in Intl Conf. on Information Technology, 2014, pp. 184–189.

[31] A. Chonka, Y. Xiang, W. Zhou, and A. Bonti, “Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks,” J. Netw. Comput. Appl., vol. 34 (4), July 2011, pp. 1097–1107.

[32] A. Mitrokotsa and C. Douligeris, “Detecting denial of service attacks using emergent self-organizing maps,” 5th IEEE Intl. Sym. on Signal Processing and Information Technology, 2005, pp. 375–380.

[33] Y. Wang, C. Lin, Q.-L. Li, and Y. Fang, “A queueing analysis for the denial of service (DoS) attacks in computer networks,” Comput. Networks, vol. 51 (12), Aug 2007, pp. 3564–3573.

[34] R. Ranchal, B. Bhargava, L. Ben Othmane, L. Lilien, A. Kim, M. Kang, and M. Linderman, “Protection of Identity Information in Cloud Computing without Trusted Third Party,” Third Intl. W. on Dependable Network Computing

and Mobile Systems (DNCMS 2010), New Delhi, India, Oct. 2010, pp. 368-372.

[35] What are the 5 most common attacks on websites? - Quora. [Online]. Available: https://www.quora.com/What-are-the-5-most-common-attacks-on-websites. [Accessed: 15 Mar. 2017].

[36] SaaS Vs. PaaS Vs. IaaS – An Ultimate Guide on When to Use What. Available: https://www.linkedin.com/pulse/saas-vs-paas-iaas-ultimate-guide-when-use-what-sonia-patel. [Accessed: 7 Mar. 2017]

[37] F. Greitzer, L. Kangas, C. Noonan, A. Dalton, and R. Hohimer,―Identifying at-risk employees: Modeling psychosocial precursors of potential insider threats,‖ in 45th Hawaii International Conference on System Science (HICSS), January 2012.

[38] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," IEEE INFOCOM, 2010, pp. 1–9.

[39] P.L.S. Kumari and A. Damodaram, "An Alternative Methodology for Authentication and Confidentiality Based on Zero Knowledge Protocols Using Diffie-Hellman Key Exchange," Intl. Conf. on Information Technology, 2014, pp. 368–373.

[40] B. Grobauer, T. Walloschek, and E. Stocker, "Understanding Cloud Computing Vulnerabilities," IEEE Secur. Priv. Mag., vol. 9 (2), Mar. 2011, pp. 50–57.

[41] G.-J. Ahn, M. Ko, and M. Shehab, "Privacy-Enhanced User-Centric Identity Management," IEEE Intl. Conf. on Communications, 2009, pp. 1–5.

[42] A. Behl, "Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation," World Congress on Information and Communication Technologies, 2011, pp.217–222.

[43] R.K. Banyal, P. Jain, and V. K. Jain, "Multi-factor Authentication Framework for Cloud Computing," in 5th Intl. Conf. on Computational Intelligence, Modelling and Simulation, 2013, pp. 105–110.

[44] H. Chen, Y. Xiao, X. Hong, F. Hu, and J. (Linda) Xie, "A survey of anonymity in wireless communication systems," Secur. Commun. Networks, vol. 2 (5), Sept. 2009, pp. 427–444.

[45] M. Despotović -Zrakić, V. Milutinović, and A . Belić, "Handbook of research on high performance and cloud computing in scientific research and education," IGI-Global, Mar. 2014.

[46] R.L. Krutz and R.D. Vines, "Cloud security : a comprehensive guide to secure cloud computing," Wiley, 2010.

[47] S.K. Das, K. Kant, and N. Zhang, "Handbook on securing cyber-physical critical infrastructure," Morgan Kaufmann, 2012.

[48] C. Phua, "Protecting organizations from personal data breaches," Comput. Fraud Secur., vol 1, Jan. 2009, pp. 13–18.

[49] N. Attrapadung, J. Herranz, F. Laguillaumie, B. Libert, E. de Panafieu, and C. Ràfols, "Attributebased encryption schemes with constant-size ciphertexts," Theor. Comput. Sci., vol. 422, Mar. 2012, pp. 15–38.

[50] F. Sabahi, "Virtualization-level security in cloud computing," IEEE 3rd Intl. Conf. onCommunication Software and Networks, pp. 250–254, 2013.