VFAST Transactions on Software Engineering
http://vfast.org/journals/index.php/VTSE@ 2021, ISSN(e): 2309-3978, ISSN(p): 2411-6246
Volume 9, Number 1, January-March 2021 *pp:30*

Security Problems in Service Delivery Models of Cloud Computing - A Survey

Mazhar Iqbal Noor

Department of Computer Science, University of Management & Technology, Lahore-Pakistan
Email: mazhar_99uet@yahoo.com

ABSTRACT
Cloud Computing has remarkable potential to provide the required services to their customers and end users with the flexible manner and in minimal cost. Cloud Computing is an efficient process to accelerate the capability or increase capacity without adding in new infrastructure. It provides support and training to new persons and gives license for new software. To explore the concept services on-demand and resources, everyone is shifting to distributive but safe environment. The major demand of end user is to access the reliable data in minimum time. Security is the major concern for this new vision of computing capability. It elaborates the Information Technology's (IT) future vision. In some previous years, the concept of Cloud Computing is the fast increasing idea in IT business. But when companies place their data in cloud, they are so conscious about the environment that how much it will safe as compared to their local data centers. End users of Cloud service must understand the risks. In my survey paper, a discussion about security risks which a user may be faced. Data Security has been mainly discussed because validity of data is so important for cloud customers. This paper present a detailed overview of the security issues of different aspects affecting cloud computing. Furthermore, a comprehensive and brief discussion on several key components regarding applications, embedded system, storage system, clustering and other inter related issues. Additionally, it describes the requirements for the best security measurement.

KEYWORDS
Cloud computing, cloud service, cloud service description, SaaS service, PaaS service, IaaS service, USDL, Data privacy, Data protection, Security Virtualization

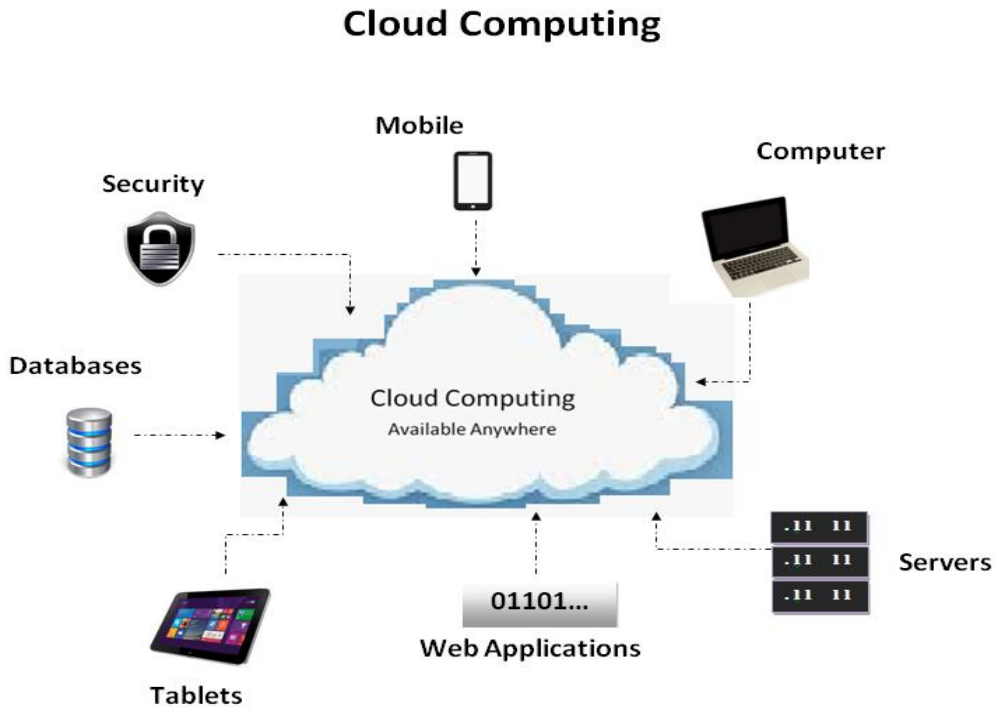
JOURNAL INFO
HISTORY: Received: February 15, 2021 Accepted: March 15, 2021 Published:..March 30, 2021

1. INTRODUCTION

Cloud computing is an internet based resources that are provided to the users on request. It is a model for accessing the resources like data storage, server computers, computer software and other applications. A number of services are offered by Cloud computing which are usually divided into three layers:

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

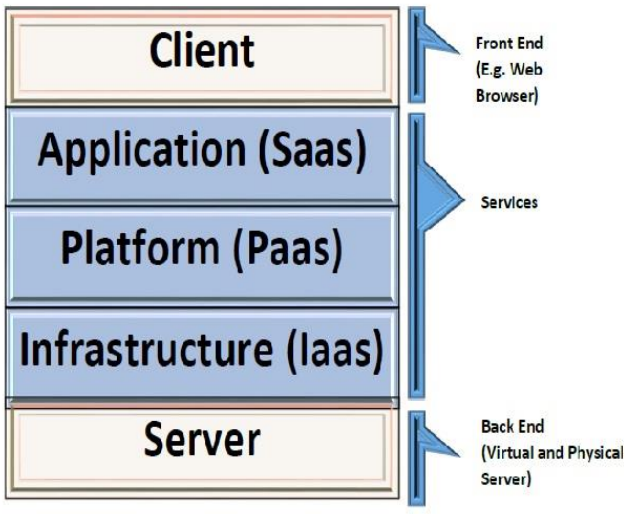
These cloud services are provided to consumers via internet. A number of cloud service providers (Google, Microsoft Azure, Amazon, etc.), which are in competition to make strength & increase the number of cloud services. Cloud computing is a well-known model for provided the services where computing arrangement are delivered as service [1]. According to Gartner's hype cycle for promising technology 2010, it has moved the heights of anticipations and will accepted by organizations within two to five years [2]. With the help of technology, there are more complications and challenges. Data security and confidentiality are the major problems in adopting the service of cloud at the enterprise level [3-5]. Cloud Computing services are dispersed by a service provider to clients for a defined period with pricing structures, SLA (Service Level Agreement), and legal agreement is written between both the parties and bounded them in the cloud service life cycle. These business bindings should be defined in the CSD(Cloud Service Description).As huge data cloud computing and internet technologies are growing, they suggest a new concept of services. These online activities are interconnected by these new services. By the reference of a survey from Cisco, the Internet of Things (IoT) is gradually growing the capabilities of the cloud. A number of researches show that there are three major delivery models like IaaS, PaaS, and SaaS. Many service models are present with respect to their performance, functionality and service delivery capabilities. Cloud computing may be compared to some other technologies which may be named as: Utility computing, Grid computing, and Autonomic computing [9]. Scientist have used mathematical modeling to invent solution to computational problems [21-51].



(Figure 1: Structure of Cloud Computing)

(Figure 1. depicts the cloud computing structure as shown above in which all the devices interact with each other and with clouds for the purpose of data sharing, software development and database access etc.)

(Cloud Service Stack)



(Figure 2: Services of Cloud are provided in the form of IaaS, PaaS, SaaS.)

History of Cloud Computing: The origin of this term is not clear. The word "cloud" is used in the domain of internet and it has a cloud-like shape to represent a network. Then it was used to depict the Internet in the diagrams of computer network. The symbol of cloud was used to indicate networks of computing equipment by ARPANET in 1977 and by CSNET in 1981.

In early 1960s, time-sharing systems introduced via RJE (Remote Job Entry). In the 1990s, some telecom companies offered dedicated point-to-point circuits for data and introduced virtual private network (VPN) services at a lower cost. Since 2000, the concept of cloud computing started.

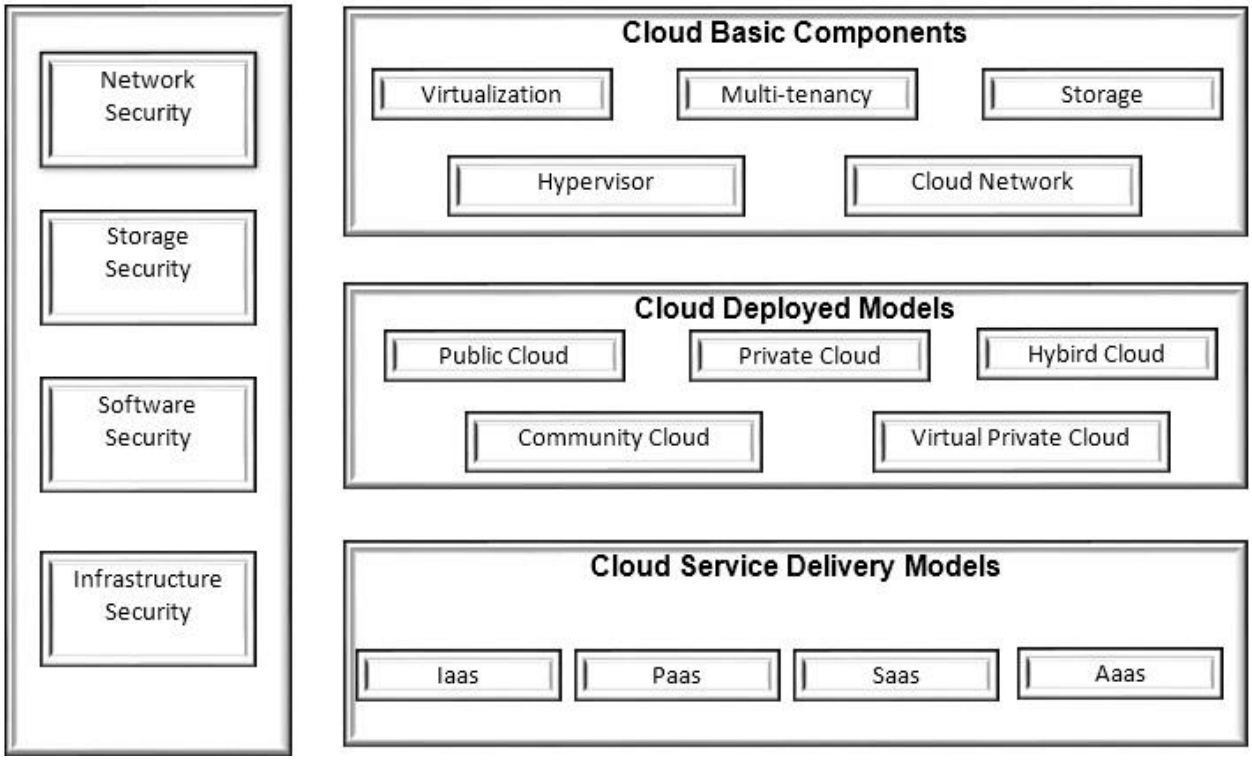
Literature Review: We recommend a Systematic Literature Review (SLR) to collect and consider all the studies available on a service depiction in cloud computing. Specially, the consideration of salient features of papers is a major part of Research Methodology. All the individualities will be explored. We selected the papers published from 2012 to 2016. These papers were selected from different journals. All the Studies that are not linked to the composition of cloud computing were rejected and removed. In present work, I did work by searching journals, workshops, books from Google Scholar and some scientific databases like IEEE, Springer Link, and Science Direct etc). Irrelevant studies and materials which I was collected were excluded according to the titles, abstracts and analysis. After the filtration of publications list by reading titles, keywords and abstracts, the

selected article was read comprehensively. In order to ensure that the content is related to our research topic. Finally, 15 studies were selected from 2012 to 2016. We read and analyze these studies carefully and with full attention then start writing my survey paper.

Components of Cloud Computing: We will discuss here the basic components on which the Cloud Computing deployed. It consists of a lot of services that we can use across the internet. We will discuss some of them which are very important.

- **Multi-Tenancy**: The Multi-tenant environment have a large number of users or customers who have no access to see the data of each other but users can share the application and resources in an execution environment, although did not belong to the same business organization. The results of Multi-tenancy environment are optimal and there is maximum utilization of hardware and data storage techniques.
- **Virtualization:** This component performs a major function in deploying the cloud. It is the planned component in the cloud computing, which permits the physical resources shared by multiple consumers. It develops and creates the virtual instance of each resource such as servers, operating system, storage devices and network resources.
- **Cloud Storage**: This is also an important component, which is managed, maintained and remote back up is done. It is available across the network where the consumers or users can access their data easily.
- **Cloud Network**: It consists of multiple data centers. A number of servers are available in a data centre. Cloud networking is required for secure and efficient sharing network and storage devices. Internet connection is required which enables the users to access the printers, storage devices or any other application in a secured environment.
- **The Hypervisor**: This manager or virtual machine monitor is an important key module of virtualization. It permits various Virtual Machines to run on a single hardware host. It monitors and manages the various operating systems, which run in a common physical system

Cloud Computing Framework



(Figure 3: Detail of Cloud Basic Components, Deployed Models and Service Delivery Models)

Cloud Deployed Models: Cloud Computing bring the challenges and security risk for IT management. This is very expensive to deal with these issues [6]. Organization focus on cloud computing models of deployment to control the operating cost. Therefore the selection of deployment models which are available on cloud is very important for a business

organization. Figure 3 depicts and explains the cloud deployed models.

- Private Cloud
- Public Cloud
- Hybrid Cloud

Private Cloud: When a single organization manages the cloud computing, whether self or from other party and may be hosted by itself or outside firm. Private cloud does not bring due to its cost. It is compared to buy his infrastructure. At initial stage, organizations face the challenges and have some major reservations regarding data security[20]. These concerns are removed by giving hosting is done for a client and the required structure for hosting may be on premises or outside the premises. In private cloud, it is easier to recognize the customer and seller relationship because the infrastructure which is required is owned and controlled by the single organization. Cloud computing is dependent on shared resources by local servers. Therefore, it is able to maintain consistency by acquiring the benefit of resource sharing.

Public Cloud: In a public cloud, all the required services are provided on to computer network that is free for general public use. There is no big difference in both the cloud structure. In public cloud, user and service provider have a strong Service Level Agreement (SLA) to establish a trust between them. In public cloud, open access to the user and other business organization is provided. Government, Businesses and academic organizations own public cloud environments. Normally cloud service providers like Google, Microsoft offer the free services at their established data centers and the open access is possible through Internet. This is the suitable model for business persons who use these services free of cost which are used by multiple users otherwise they need highly budget for this kind of infrastructure. This model also reduces the capital cost.

Hybrid Cloud: Hybrid Cloud is a merged product of both the clouds. The applications and the data are bounded together by standardized technology. Hybrid cloud has the capacity to provided the services with the resources of clouds. It provides the advantages of multiple clouds deployment models. It is secure and well organized than public cloud while receiving the entities over the internet. This model helps business organizations to get benefit of data hosting and fully managed and secured applications.

Cloud Service Delivery Models and their Security Issues: Big Data Cloud Computing and Internet technology grow; they float a new and unique concept of services. These services interconnect the increasing number of online aaS.

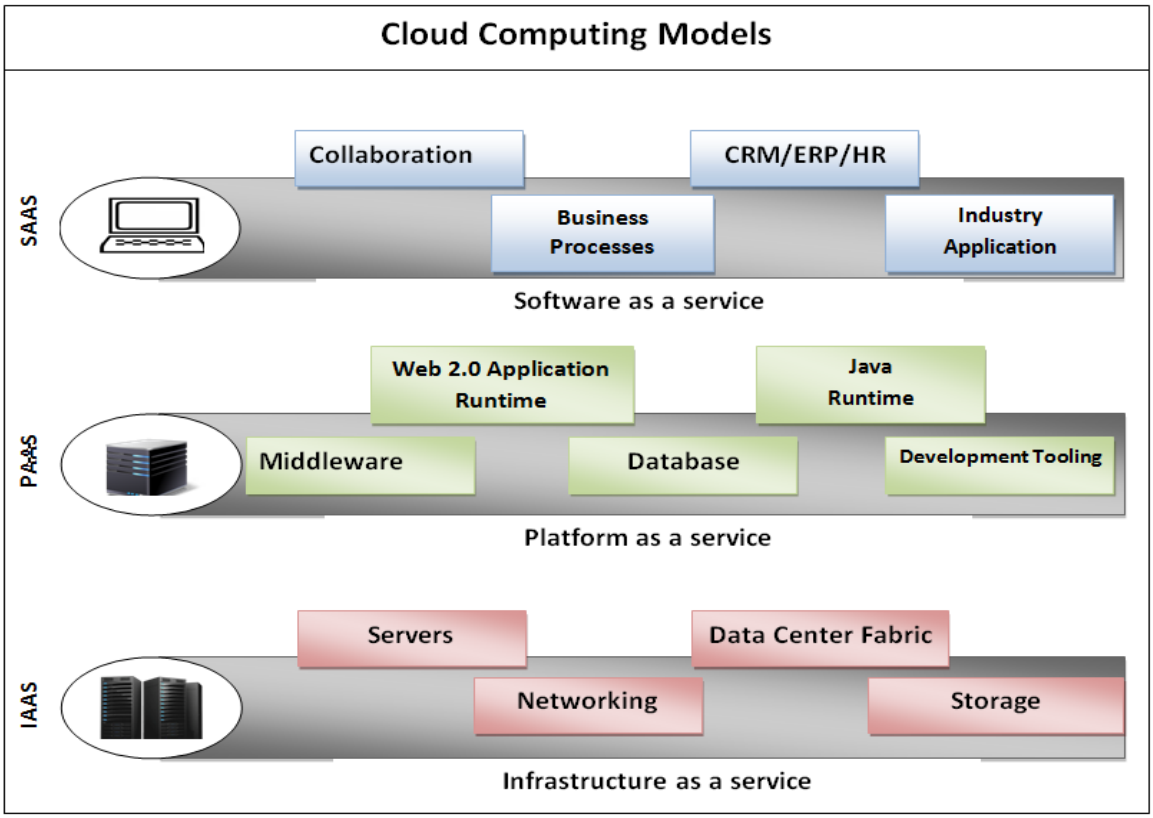
activities [12]. With the reference of survey by Cisco, the Internet of Things (IoT) is gradually increasing the capabilities of the cloud. After a large number of researches, the service delivery models are PaaS, IaaS and SaaS.

Infrastructure as a service (IaaS): *It* is the bottom of Service Delivery Model. IaaS deals with hardware (Processor, Network Storage, Data Center, virtual Server Machine and Memory) as a service. Cloud infrastructure does not control by the consumer but it possesses control over storage and applications. IaaS supports the business investment in Information Technology infrastructure. The allocation of virtual or physical resources helps in providing the infrastructure. It also provides provisions (such as hypervisor) basic issues of infrastructure without the spending huge amount of funds and time. IaaS also visualize the security issues like firewall, intrusion detection etc [8]. However, IaaS has a large number of security issues till today.

Security Problems of IaaS: In Infrastructure as a Service, the application designer has reliable control over the security. The second step is reliable data which is saved in hardware of service provider. Owner of data should hold and control over data. Different techniques are used to gain the trust on the security offered by a cloud service provider. For example, it's a vendor responsibility to provide security from each side.

Platform as a service (PaaS): Platform as a service is a middleware of service model and it provides the services in the shape of frameworks, operating systems, database environment, (IDE) and programs. The client control the applications but do not know that how the resources are managed. It may be so helping where number of developers is working at different locations but they work together. A famous *PaaS* source is Google App Engine. Google App Engine is a Development Kit which provides a platform that supports Java, Python etc. It also provides multiple features for the customer, and it is more flexible than SaaS model. In PaaS, at runtime and the time of deployment of applications, security is compromised. It also has some more major challenges like the relationship with the third party. Developers develop the applications and run the solutions without paying any cost. PaaS initiates programming environments to utilize application. Such kind of programming environments has a positive impact such as rules on which application can demand from an Operating system [6].

Security problems in PaaS: In PaaS, the provider of service switches the control to the user to design applications at this platform. Application security level such as network and host will be in the scope of the service provider. He has to make sure that the data will never be accessible to other programs and applications. This model makes enable to developers to design their own applications using this platform. As a result it is more extensible than S



(Figure 3: Cloud Computing Service Delivery Models)

Software as a service (SaaS): SaaS is a package of remote cloud services. Among delivery models, it is at the top of list. It permits the remotely deployment of applications by third-party vendors. It also allows the users to use the services of cloud infrastructure via the internet. In this model, user gains the remote access to databases and application software. In the SaaS model, cloud suppliers operate the software in the cloud and also users have the access of application or software. It is not the responsibility of Cloud users to manage the platform where the software and application runs. Thus there is no requirement to install the applications on the user's personal computer. This is a clean process for the user. Client is totally dependent on the provider of service for data accuracy and proper security. The service provider is very reluctant because there may be different users on the network which access the data at the same time but data of each user should be confidential and does not access to any other user. And it is more difficult for the user to ensure that proper security is done and application will be easily available when user needed.

Cloud Data Storage: It is a cloud service where data is remotely stored, maintained, managed, and backed up. Storage services are such as Amazon's S3 and Microsoft's Azure allow users to send their information to the cloud and they neglect the maintaining expanses to make a building and a private storage infrastructure. Several benefits such as the reliability and availability are available at a relatively low cost [13].

Security Problems in SaaS:

Following are the major areas where we can measure security .

- **Data Security**
- Computer Network
- Location of Data
- Segregation of Data
- Authentication and Authorization
- Confidentiality of Information
- Availability
- Backup

These are the different security issues in SaaS but we will discuss data security in detail in our paper [17][18]. **Security of Data** in cloud computing is main concern because data storage is the need of every organization and a user. Data security is a big issue in distributed system and online application. Each organization stores its sensitive data within its boundary. There are different policies that are subject to its logical and physical for access control. In this model, the organization stores its data outside the boundary. SaaS service provider must ensured security checks. This measurement involves the strong encryption procedures for the security of data.

Availability of data: Data is very important for everyone and the main target of cloud service is also to ensure high

availability of data to the client. It means that at any time and anywhere when the client is required his data, it should be available to him. Hardware should be provided as demanded by the authorized user. Some of the time cloud storage fails in the availability of some attributes because of flooding attack in the network. System availability means to carry on working and operations even when some establishment misbehaves [18].

Anonymity: It is process or a technique to obscure the available data and key information which prevents the identity of the owner of data. In the clouds, it is increasing to have ambiguity without the measurement of privacy which may be causes de-anonymity attack. Data anonymity has different loopholes, threats in the process of re-identification.

Data warehouse: These are very large system and offering to different communities of users according to their security needs. Security is the major requirement for the deployment of DWH. Cong W. et al. said that security has always been an important part of QoS (Quality of Service) There are three major security issue in Data warehouse i.e. Confidential, integrated and available data.

Data loss and leakage*: D*ata loss may occur when disk drive dead without making any backup. This is the lack of privacy and impacts on SLA policy, which are the main problems of users. The data leakage directly effects the web application and attacker gets the advantage and got permission in cloud implementations [19].

Integrity and confidentiality issues: Three major challenges are present for cloud storage, integrity, confidentiality, and availability (CIA).Availability of data that we have discussed earlier. We will discuss here confidentiality and integrity. **Integrity** is the most important in system information to protect the data from unauthorized changes, deletion or alteration.

Cong Wang suggested a way from mathematics to prove the integrity of the data [7]. Integrity is a process to protect the data from illegal deletion or fabrication [15].

Confidentiality is a security issue. Measures to ensure that sensitive information will never access to the wrong people and it must sure that the right people can get the information.

Authorization is the process to establish the level of access for an authenticated user [13].

Inference: Inference is a technique used to attack the databases where illegal users try to access the sensitive and important information from databases at a high level. Inference is also a technique of data mining which is used to take information hidden from normal users. An inference attacker can access an entire database. We have to implement the security according to the complexity of database. If the problems of inference are not solved efficiently then the sensitive information may be accessed and copied to unauthorized users.

Cryptography*:* cryptography is a technique for constructing protocols that prevents the unauthorized users to access and read private messages of others. Modern cryptography includes major modules in information security such as data integrity, data confidentiality and authentication [14]. Cryptography also includes passwords, military communications, electronic commerce, ATM cards etc [10].

Cryptography is conversion of data or information from a readable state to such state that is not readable to third party. Original owner of data can read this information by decryption method. No one can decrypt the data without a key. Most of the times in cryptographic algorithms near to fail when the security measure are applied. In cloud cryptography, many algorithms and protocols are applied to minimize and overcome the security issues but it has many other challenges still now to overcome. Poor computation efficiency, key management is also other issues related to cloud cryptography. **Symmetric-key cryptography** is a type in which a key is shared between the sender and receiver. In **Public key cryptography**, a pair of key is used. Public key which may be known to everyone but private keys that are known only to the owner.

Cryptographic Cloud Storage: Kamara and Lauter [11] recommended a virtual private storage services that would satisfy the user demands. These demands are performed by encrypting the documents available in the cloud.

Cryptographic Architecture for Cloud Storage: This includes three stages.

(1) Processor of Data, which interprets the data prior to send it.
(2) Verification of Data which ensures integrity of data.
(3) Generation of Token, which produces tokens by giving permission to the service provider.

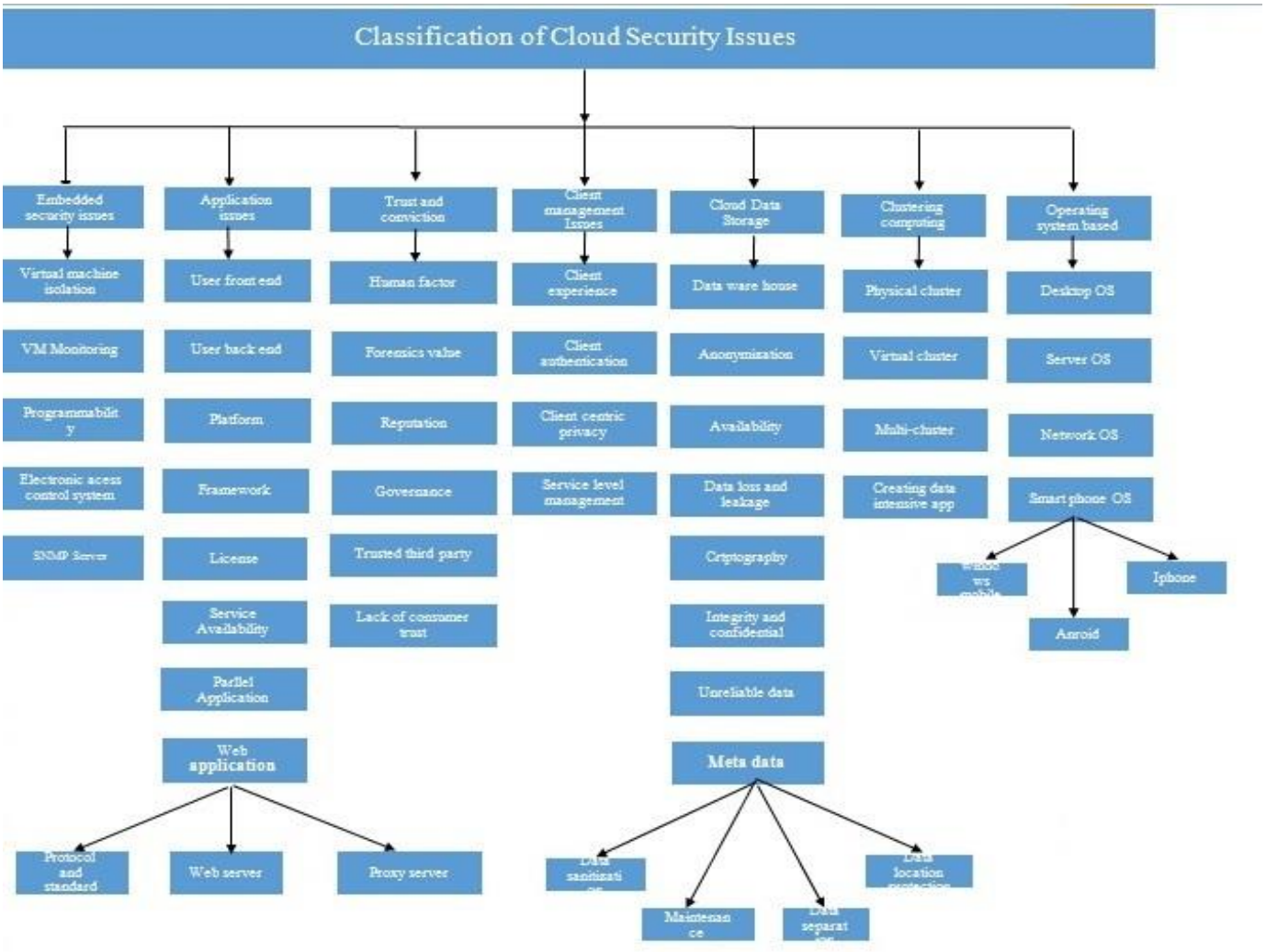


Figure 4: Classification of cloud security issues

CONCLUSION: It's a big true that cloud computing has a large number of benefits but still there are so many difficulties which we have to solve. Cloud computing can provide multiple advantages to organizations. If we estimate the revenue then it is true that cloud computing is a favorable industry for income generation. Everyone wants to generate more and more revenue with minimum input. The use of cloud computing is very common in organizations but it may be increase if the trust level of customer increases by giving them guarantee for data security. There are chances of more threats from hackers. The major issue and challenge for cloud computing is the data security in the cloud environment, different techniques, approaches and models have already been suggested and proposed by different researchers. Services providers of cloud computing are now exploring the proper privacy and security mechanisms which would make the cloud environment safe. Their customers should keep full trust and faith on the clouds. In this survey paper, we have discussed the techniques and cryptographic storage technology in clouds. As we see in our survey paper that security threats are the main issues which we have to be solved then we can gain the trust of client. Every client of cloud computing want the privacy of his data from others users and applications. The main concern is that who is accessing the information on the internet.

Future Work: I have completed the survey. To manage security problems at different cloud layers but we have also identified some challenges and difficulties for future. It gives us provision for future work. In future we can study existing techniques and may explore of new techniques for security in clouds. Challenges may change day by day. There is a major responsibility of the governments to make standards and policies for the data privacy and security. The level of trust on cloud vendors will be increased when the satisfaction level of cloud customer will increase.

REFERENCES:

[1] Modi, C., Patel, D., Borisaniya, B., Patel, A., & Rajarajan, M. (2013). A survey on security issues and solutions at different layers of Cloud computing. *The journal of supercomputing*, *63*(2), 561-592.

[2] Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications*, *34*(1), 1-11.

[3] Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation computer systems*, *28*(3), 583-592.

[4] Iankoulova, I., & Daneva, M. (2012, May). Cloud computing security requirements: A systematic review. In *2012 Sixth International Conference on Research Challenges in Information Science (RCIS)* (pp. 1-7). IEEE.

[5] Popović, K., & Hocenski, Ž. (2010, May). Cloud computing security issues and challenges. In *The 33rd international convention mipro* (pp. 344-349). IEEE.

[6] Takabi, H., & Joshi, J. B. D. Gail-Joon Ahn, 2010,". *Security and Privacy Challenges in Cloud Computing*.

[7] Chen, D., & Zhao, H. (2012, March). Data security and privacy protection issues in cloud computing. In *2012 International Conference on Computer Science and Electronics Engineering* (Vol. 1, pp. 647-651). IEEE.

[8] Bhadauria, R., Chaki, R., Chaki, N., & Sanyal, S. (2011). A survey on security issues in cloud computing. *arXiv preprint arXiv:1109.5388*, 1-15.

[9] Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. J Internet Serv and Appl 1: 7–18.

[10] Hussein, N. H., Khalid, A., & Khanfar, K. (2016). A survey of cryptography cloud storage techniques. *International Journal of Computer Science and Mobile Computing*, *5*(2), 186-191.

[11] Jasim, O. K., Abbas, S., El-Horbaty, E. S. M., & Salem, A. B. M. (2013). Cloud Computing Cryptography" State-of-the-Art. *International Journal of Computer, Control, Quantum and Information Engineering*, *7*(8), 524-527.

[12] Takabi, H., Joshi, J. B., & Ahn, G. J. (2010). Security and privacy challenges in cloud computing environments. *IEEE Security & Privacy*, *8*(6), 24-31.

[13] Kamara, S., & Lauter, K. (2010, January). Cryptographic cloud storage. In *International Conference on Financial Cryptography and Data Security* (pp. 136-149). Springer, Berlin, Heidelberg.

[14] Nithiavathy, R. (2013, February). Data integrity and data dynamics with secure storage service in cloud. In *2013 International Conference on Pattern Recognition, Informatics and Mobile Engineering* (pp. 125-130). IEEE.

[15] Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation computer systems*, *28*(3), 583-592.

[16] Jain, N., & Kaur, G. (2012). Implementing DES algorithm in cloud for data security. *VSRD-IJCSIT*, *2*(4), 316-321.

[17] Bhadauria, R., Chaki, R., Chaki, N., & Sanyal, S. (2014). SECURITY ISSUES IN CLOUD COMPUTING. *Acta Technica Corvininesis-Bulletin of Engineering*, *7*(4).

[18] Tripathi, P., & Suaib, M. (2014). Security Issues On Cloud Computing. *International Journal of Engineering Technology, Management and Applied Sciences*, *2*(6).

[19] Chen, D., & Zhao, H. (2012, March). Data security and privacy protection issues in cloud computing. In *2012 International Conference on Computer Science and Electronics Engineering* (Vol. 1, pp. 647-651). IEEE.

[20] Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information sciences*, *305*, 357-383.

[21] Khan, Y. D., Ahmad, F., & Anwar, M. W. (2012). A neuro-cognitive approach for iris recognition using back propagation. *World Applied Sciences Journal*, *16*(5), 678-685.

[22] Ahmad, F., Fakhir, I., Khan, S. A., & Khan, Y. D. (2014). Petri net-based modeling and control of the multi-elevator systems. *Neural Computing and Applications*, *24*(7-8), 1601-1612.

[23] Khan, Y. D., Ahmad, F., & Khan, S. A. (2014). Content-based image retrieval using extroverted semantics: a probabilistic approach. *Neural Computing and Applications*, *24*(7-8), 1735-1748.

[24] Khan, Y. D., Ahmad, F., & Khan, S. A. (2013). A Survey on use of Neuro-Cognitive and Probabilistic Paradigms in Pattern Recognition. *Research Journal of Recent Sciences*, *2*(4), 74-79.

[25] Akmal, M. A., Rasool, N., & Khan, Y. D. (2017). Prediction of N-linked glycosylation sites using position relative features and statistical moments. *PloS one*, *12*(8), e0181966.

[26] Ehsan, A., Mahmood, K., Khan, Y. D., Khan, S. A., & Chou, K. C. (2018). A novel modeling in mathematical biology for classification of signal peptides. *Scientific reports*, *8*(1), 1-16.

[27] Khan, Y. D., Rasool, N., Hussain, W., Khan, S. A., & Chou, K. C. (2018). iPhosT-PseAAC: Identify phosphothreonine sites by incorporating sequence

statistical moments into PseAAC. *Analytical biochemistry*, *550*, 109-116.

[28] Khan, Y. D., Batool, A., Rasool, N., Khan, S. A., & Chou, K. C. (2019). Prediction of nitrosocysteine sites using position and composition variant features. *Letters in Organic Chemistry*, *16*(4), 283-293.

[29] Butt, A. H., Rasool, N., & Khan, Y. D. (2018). Predicting membrane proteins and their types by extracting various sequence features into Chou's general PseAAC. *Molecular biology reports*, *45*(6), 2295-2306.

[30] Ghauri, A. W., Khan, Y. D., Rasool, N., Khan, S. A., & Chou, K. C. (2018). pNitro-Tyr-PseAAC: predict nitrotyrosine sites in proteins by incorporating five features into Chou's general PseAAC. *Current pharmaceutical design*, *24*(34), 4034-4043.

[31] Khan, Y. D., Jamil, M., Hussain, W., Rasool, N., Khan, S. A., & Chou, K. C. (2019). pSSbond-PseAAC: Prediction of disulfide bonding sites by integration of PseAAC and statistical moments. *Journal of theoretical biology*, *463*, 47-55.

[32] Khan, Y. D., Rasool, N., Hussain, W., Khan, S. A., & Chou, K. C. (2018). iPhosY-PseAAC: identify phosphotyrosine sites by incorporating sequence statistical moments into PseAAC. *Molecular biology reports*, *45*(6), 2501-2509.

[33] Hussain, W., Khan, Y. D., Rasool, N., Khan, S. A., & Chou, K. C. (2019). SPalmitoylC-PseAAC: A sequence-based model developed via Chou's 5-steps rule and general PseAAC for identifying S-palmitoylation sites in proteins. *Analytical biochemistry*, *568*, 14-23.

[34] Khan, S. A., Khan, Y. D., Ahmad, S., & Allehaibi, K. H. (2019). N-MyristoylG-PseAAC: sequence-based prediction of N-myristoyl glycine sites in proteins by integration of PseAAC and statistical moments. *Letters in Organic Chemistry*, *16*(3), 226-234.

[35] Butt, A. H., Rasool, N., & Khan, Y. D. (2019). Prediction of antioxidant proteins by incorporating statistical moments based features into Chou's PseAAC. *Journal of theoretical biology*, *473*, 1-8.

[36] Awais, M., Hussain, W., Khan, Y. D., Rasool, N., Khan, S. A., & Chou, K. C. (2019). iPhosH-PseAAC: Identify phosphohistidine sites in proteins by blending statistical moments and position relative features according to the Chou's 5-step rule and general pseudo amino acid composition. *IEEE/ACM transactions on computational biology and bioinformatics*.

[37] Rasool, N., Husssain, W., & Khan, Y. D. (2019). Revelation of enzyme activity of mutant pyrazinamidases from Mycobacterium tuberculosis upon binding with various metals using quantum mechanical approach. *Computational biology and chemistry*, *83*, 107108.

[38] Rehman, K. U. U., & Khan, Y. D. (2019). A Scale and Rotation Invariant Urdu Nastalique Ligature Recognition Using Cascade Forward Backpropagation Neural Network. *IEEE Access*, *7*, 120648-120669.

[39] Butt, A. H., & Khan, Y. D. (2019). Prediction of S-Sulfenylation sites using statistical moments based features via Chou'S 5-Step rule. *International Journal of Peptide Research and Therapeutics*, 1-11.

[40] Ilyas, S., Hussain, W., Ashraf, A., Khan, Y. D., Khan, S. A., & Chou, K. C. (2019). iMethylK-PseAAC: Improving Accuracy of Lysine Methylation Sites Identification by Incorporating Statistical Moments and Position Relative Features into General PseAAC via Chou's 5-steps Rule. *Current Genomics*, *20*(4), 275-292.

[41] Barukab, O., Khan, Y. D., Khan, S. A., & Chou, K. C. (2019). iSulfoTyr-PseAAC: Identify tyrosine sulfation sites by incorporating statistical moments via Chou's 5-steps rule and pseudo components. *Current Genomics*, *20*(4), 306-320.

[42] Khan, Y. D., Amin, N., Hussain, W., Rasool, N., Khan, S. A., & Chou, K. C. (2020). iProtease-PseAAC (2L): A two-layer predictor for identifying proteases and their types using Chou's 5-step-rule and general PseAAC. *Analytical biochemistry*, *588*, 113477.

[43] Malebary, S. J., Rehman, M. S. U., & Khan, Y. D. (2019). iCrotoK-PseAAC: Identify lysine crotonylation sites by blending position relative statistical features according to the Chou's 5-step rule. *PloS one*, *14*(11), e0223993.

[44] Butt, A. H., & Khan, Y. D. (2019). CanLect-Pred: A Cancer Therapeutics Tool for Prediction of Target Cancerlectins Using Experiential Annotated Proteomic Sequences. *IEEE Access*, *8*, 9520-9531.

[45] Akmal, M. A., Hussain, W., Rasool, N., Khan, Y. D., Khan, S. A., & Chou, K. C. (2020). Using Chou's 5-steps rule to predict O-linked serine glycosylation sites by blending position relative features and statistical moment. *IEEE/ACM Transactions on Computational Biology and Bioinformatics*.

[46] Hussain, W., Rasool, N., & Khan, Y. D. (2020). A Sequence-Based Predictor of Zika Virus Proteins Developed by Integration of PseAAC and

Statistical Moments. *Combinatorial chemistry & high throughput screening*, *23*(8), 797-804.

[47] Hussain, W., Rasool, N., & Khan, Y. D. (2020). Insights into Machine Learning-based approaches for Virtual Screening in Drug Discovery: Existing strategies and streamlining through FP-CADD. *Current Drug Discovery Technologies*.

[48] Shah, A. A., & Khan, Y. D. (2020). Identification of 4-carboxyglutamate residue sites based on position based statistical feature and multiple classification. *Scientific Reports*, *10*(1), 1-10.

[49] Amanat, S., Ashraf, A., Hussain, W., Rasool, N., & Khan, Y. D. (2020). Identification of Lysine Carboxylation Sites in Proteins by Integrating Statistical Moments and Position Relative Features via General PseAAC. *Current Bioinformatics*, *15*(5), 396-407.

[50] Mahmood, M. K., Ehsan, A., Khan, Y. D., & Chou, K. C. (2020). iHyd-LysSite (EPSV): Identifying Hydroxylysine Sites in Protein Using Statistical Formulation by Extracting Enhanced Position and Sequence Variant Feature Technique. *Current Genomics*, *21*(7), 536-545.

[51] Naseer, S., Hussain, W., Khan, Y. D., & Rasool, N. (2020). iPhosS (Deep)-PseAAC: Identify Phosphoserine Sites in Proteins using Deep Learning on General Pseudo Amino Acid Compositions via Modified 5-Steps Rule. *IEEE/ACM Transactions on Computational Biology and Bioinformatics*.