# An Innovative Model for both Cloud Security and Privacy in Provision of Secure Cloud Services

**Gouni Ritthiika Reddy, Devavarapu Sreenivasarao, Shaik Khasim Saheb**

***Abstract*: Because of diverse benefits such as counting services on demand, decreasing costs, computing resources configuration, flexibility, services scalability, etc. over internet, Cloud Computing has become and is becoming widely and hugely accepted technology to provide services. On the other hand, privacy and security of a cloud has become an issue as this technology is tremendously emerging in the world. Many researches are being done and even some proposed various models to identify and overcome the privacy and security issues. In this review, for the cloud providers to use during different stages of cloud services, a layered cloud security and privacy model (CSPM) will be provided. The CSPM model allows to overcome cloud security issues and thus, providing safe and protected services. Lastly, countermeasures and security threats will be presented.***

***Keywords*: Privacy, Cloud Provider, Cloud Security and Privacy Model (CSPM), Cloud Service, Data, Cloud Consumer, Security, Cloud Computing.***

## I. INTRODUCTION

For accessing data and programs, storing data over the internet, cloud computing is mainly used and it is generally referred as “cloud”. It makes the data available for the users over the internet. To a single organization or maybe for more than one organization, access of cloud may be restricted. As per the proponents, cloud computing permits receiving their applications up and boosting them, simultaneously managing them effectively with less maintenance and allowing IT teams to accommodate themselves to the inconsistent and indeterminate demand, a “pay as you go” model, a maybe cause for sudden prices of operating when unknown expense models of cloud are used by the administrators, is used by cloud providers.

As per NIST, cloud computing is made of four deployment models and 3 service models. Public, Community, Private and Hybrid are the deployment models of the cloud. Moreover, on demand self-service, calculated service, resource pooling, rapid flexibility and broad network access are the five characteristics that differentiate cloud from different technologies [1]. Computing needs of a cloud computing model supported by software and hardware components refer to a cloud infrastructure. As mentioned above, the service models i.e. the three models form the infrastructure of cloud.

## II. CLOUD SERVICE MODELS

The cloud service models are as follows.

- Software as a Service
- Platform as a Service
- Infrastructure as a Service

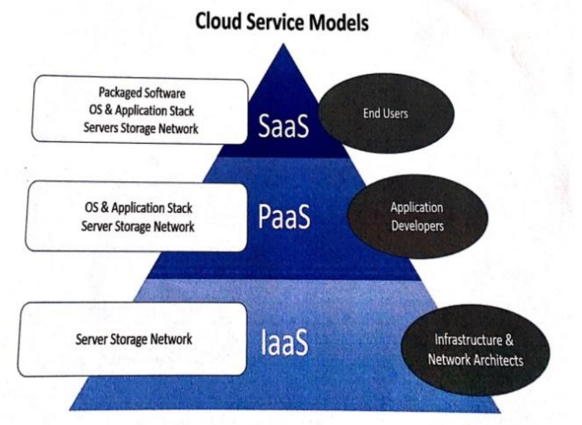


**Fig. 1. Various Models of Cloud Services**

### A. Infrastructure as a Service

The first and foremost layer in the cloud architecture is IaaS(Infrastructure as a Service). For developing and deploying the applications, this service provides the user the infrastructure. That may include storing data, firewall and load balancer. The IaaS service creates a cloud infrastructure for computing applications.

### B. Platform as a Service

This is the second layer of cloud architecture. Using this service, the programmers will program the cloud with an infrastructure. This service provides various programming models, languages and frameworks to make the cloud programmable.

Revised Manuscript Received on November 30, 2019.
* Correspondence Author

**Gouni Ritthiika Reddy***, Department of Computer Science & Engineering, Sreenidhi Institute of Science and Technology, Telangana, India. E-mail: ritikareddy.g@gmail.com

**Devavarapu Sreenivasarao,** Assistant Professor, Department of Computer Science & Engineering Department, Sreenidhi Institute of Science and Technology, Telangana, India. E-mail: sreenivasaraodevavarapu@gmail.com

**Shaik Khasim Saheb,** Assistant Professor, Department of Computer Science & Engineering Department, Sreenidhi Institute of Science and Technology, Telangana, India. E-mail: shaikkhasims@sreenidhi.edu.in

The advantage of this service is that developers can develop and run the applications without knowing the underlying features.

**C. Software as a Service**

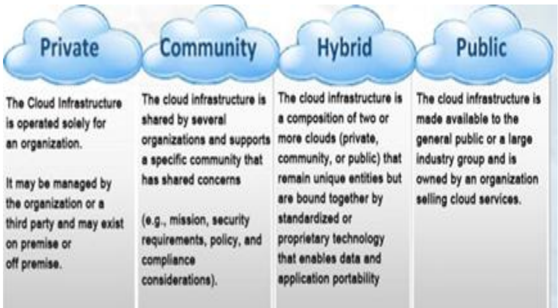
This is the 3rd layer of cloud infrastructure. This service generally provides built in applications to the user which can be accesses by them through web browser. Instagram, Face book, Twitter are the best examples for this type of service.

## III. DEPLOYMANT MODELS

According to NIST, there are 4 Deployment models

- Public
- Community
- Private
- Hybrid

All this models can be understood by using the below figure.



The Cloud Infrastructure is operated solely for an organization.

It may be managed by the organization or a third party and may exist on premise or off premise.

The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns

(e.g., mission, security requirements, policy, and compliance considerations).

The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability

The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

**Fig. 2. Deployment Models of a Cloud**

Until now, we discussed the basic infrastructure of cloud. Now, we are going to focus on the threats and attack on cloud services and models. As we know, cloud atmosphere is widely spread and highly vibrant [2]. There are many concerns about the security and privacy of cloud services. Security, privacy, data availability of cloud services can be threatened by such issues. Generally, there are two types of attacks.

### A. Insider attacks

A spiteful insider working for an organization or cloud provider and outsourcing its IT infrastructure, private data to an outsider or into the cloud are considered insider attacks.

### B. Outsider attacks

Attacks done by the adversaries that do not have direct access to any authorized information in the network. Attacks such as replay messages and eavesdropping fall into this classification. To recognize and understand cloud privacy and security issues, many researches are being and been done. They are also classified into 5 categories.

- Security standards
- Network
- Access control
- Cloud infrastructure
- Data

SMI is hierarchical and a standard measurement framework as developed by CSMIC [5]. It is classified into 7 categories. One of the seven is Privacy and security. The Privacy and security category of this structure include

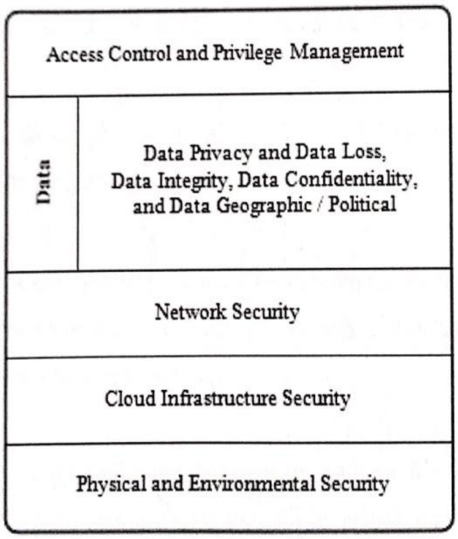
- Privilege and Access Control Management
- Physical and Environmental Security
- Proactive threat
- Data Privacy and Data Lass
- Data Geographic
- Data Integrity
- Disposition
- Security Management

Many researchers have been done and they proposed a model called cloud security and privacy model to overcome or reduce security issues of cloud services.

## IV. PROPOSAL MODEL

The CSPM is a layered model and is classified into 5 layers shown in below figure 3 [6].

The security and privacy classifications as mentioned above are used as a basis to propose CSPM model.



Access Control and Privilege Management

Data

Data Privacy and Data Loss, Data Integrity, Data Confidentiality, and Data Geographic / Political

Network Security

Cloud Infrastructure Security

Physical and Environmental Security

**Fig. 3. CSPM Model**

### A.Physical and Environmental Security Layer

The first layer of the CSPM is PESL. To look after the facilities against not permitted data, damage, physical access of the cloud providers, policies and processes are adopted by the PESL [5][6].

### B.Cloud Infrastructure Security Model

CISL is the second layer of the CSPM. Security issues concerned to cloud infrastructure is included in this layer and is also involved with virtualization environment. Security misconfiguration, insecure interface of API, multi tenancy, technical flaws etc are the security issues of the CISL layer [4][6].

### C.Network Security Layer

The third layer of CSPM is NSL. This layer generally refers to the intermediate through which the cloud users bond or interact to cloud services,

Retrieval Number: A5272119119/2019©BEIESP
DOI: 10.35940/ijitee.A5272.119119
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

such as web browsers, network connections, etc. example for this layer is the internet we use in our daily life for connecting to cloud services [4][6].

### D.Data Layer

DL is the fourth layer of CSPM. As shown in the figure 3, this layer constitutes the following components.

- **Data Geographic / Political**

Based on political and geographical risk, limitations are applied on the consumer using the location of services [5][6].

- **Data Confidentiality**

Even to the cloud provider, this layer ensures that data remains invisible. Consumer data cannot be stolen or be reused, even if the data centre of the provider has been attacked [6][8].

- **Integrity of Data**

The data is kept in its exact form which means that undue modification of information must be prevented by the system [5][6][8].

- **Privacy of Data and Data Loss**

To share and use data by the consumers, limitations are applied by the cloud providers. Report will be sent to a cloud consumer service if any failure of protection occurs [5][6].

### E. Access Control and Privilege Management Layer

The final layer of CSPM is ACPML. To ensure only consumers who are granted privileges to modify or use data, policies are adopted by the cloud providers. Policies adopted may include identification, authentication, etc. Advantages of CSPM and the benefit of its layered model are:

- To classify different privacy and security issues, CSPM can help cloud providers and researchers.
- It can help the cloud providers to differentiate between cloud threats from different sources.
- To make sure the accessibility and security of cloud services, it can assist cloud providers to take countermeasures required for each CSPM layer.
- The security and privacy monitoring of cloud services can be made easier.

## V. DISCUSSIONS AND EXPERIMENTS

### A.Contrast Experiment

Contrast Experiment has been conducted for the confirmation of contribution of CSPM.

### B. Experiment Preparation

Ten participants (ranging from 4th year undergraduates to 2nd year master students) have taken part in this experiment. Two groups were created i.e Experiment Group(EG) and Control Group(CG) and students were segregated equally. System model containing several security threats were assigned to the participants of both the groups. To recognize the privacy and security issues in the system, they were asked to use case explanation and also class diagram. Solving of identified problems was expected from the participants [14]. A privacy and security patterns were prepared as a reference and participants completed the questionnaire after completing the task they were assigned.

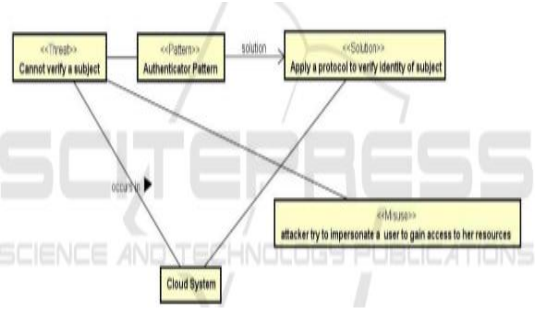


**Fig. 4. Example of the Pattern View Structure**

### C.Experiment Results

Figure 5 illustrates a box plot of experimental data which is shown in various distributions. There major variables were evaluated which includes first various patterns helpful in solving problems, various problems identified in the model, various problems cleared by just refining the model.

As per figure 5, EG was more capable at revising, even though we failed to prove difference in discovering problems. The number of revisions of Privacy and Security problems varied widely in CG, whereas students in EG revised at least 3 times. We hypothesized that CG would lag behind EG in completion of tasks. Moreover, the experimental results could not show any such variation between two groups and one of the main reason is because of more time spent by EG group in reading guidelines and meta model. All EG students gave same answers for each question when asked about their opinion on CSPM. They concluded saying that examples and explanation were useful for various pattern applications. Participants also concluded that structure of pattern view in corresponding to both Privacy and Security pattern is very useful.

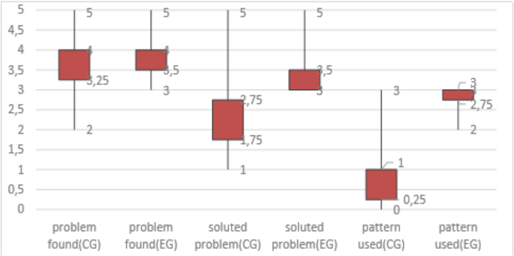


**Fig. 5. Case Study (Box plot of data)**

## VI. CASE STUDY OF TREASURE HUNTING GAME

A Case study is conducted in order to check the efficiency of the experiments which were analyzed upon considering CSPM. The case study which is conducted mainly in basis of an Android game application which uses cloud to store appropriate data. The comparative experimental results were made with existing real version of the model with the improvised version model.

### A.Preparation

Generally, privacy and security analysis is performed before designing the model. For implementing cloud function, Amazon Web Services is used in the case study chosen.

### B. Results

Based on the STRIDE model, privacy and security requirements were analyzed.

Retrieval Number: A5272119119/2019©BEIESP
DOI: 10.35940/ijitee.A5272.119119
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Threats such as listening to transmissions or tampering of data were noticed by AWS API. Thus, the following topics were given importance

### C.Authentication Problem

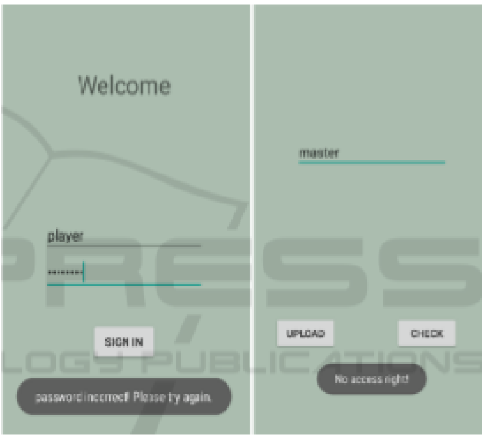
Because of lack of authentication, this particular system has high danger of individuality spoofing.

Pattern and solution: The model uses an authenticator which is added with an authenticator pattern. Before accessing the model it is required for the user to provide sign in and sign up.

### D.Access Right Problem

The users' data appears on the screen if it exists and it allows the user to check others data.

Pattern and Solution: as per role based Access control pattern, access right controller is added to access cloud storage data.



password incorrect! Please try again.

No access right!

Fig. 6. Result after pattern implementation

## VII. ATTACKS AND SECURITY THREATS OF A CLOUD

As of now, the IT world is concerned with many threats and security attacks. In the circumstances of computer security, threat refers to anything which as a calibre to cause a harm to computer system. Moreover, cloud environment is highly spread and also provides services to an ill intended person; therefore, compared to other environments cloud environment is admonitory for attacks and threats. The threats include cloud malware injection, denial in service, etc [4]. So, these threats can be insider or outsider of cloud environment, and may result in data loss, security issues, etc. here, we are going to concentrate on threats which menace the security and privacy of cloud services. The attacks and threats are in large number; thus, we will discuss some of the important threats.

### A. Insider Attacks

To make sure only authorized consumers can have ingress to the data centres of the cloud, both cloud consumers and providers must and should take up hardest policies. An official administrator can have an access to the data that he needs by either manually going on to the site or using VPN as a medium and signing-in for accessing the credentials [3]. To each and every organization system, these credentials must have to be valid for accessing. Though only authorized consumers can use the services as per the policies, an ill intended administrator working for cloud consumers or providers can misuse the privileges to illegally change data or disclose the data of the organization. This attack generally targets environmental security, cloud architecture and also the safety of system and data. Finding such attack is not an easy task because of security mechanism of organizations.

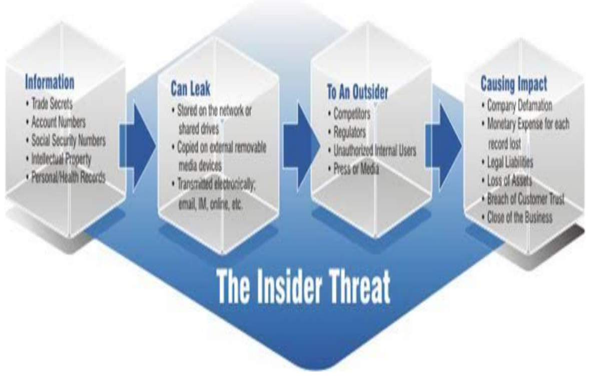

Information
• Trade Secrets
• Account Numbers
• Social Security Numbers
• Intellectual Property
• Personal/Health Records
Can Leak
• Stored on the network or shared drives
• Copied on external removable media devices
• Transmitted electronically; email, IM, online, etc.
To An Outsider
• Competitors
• Regulators
• Unauthorized Internal Users
• Press or Media
Causing Impact
• Company Defamation
• Monetary Expense for each record lost
• Legal Liabilities
• Loss of Assets
• Breach of Customer Trust
• Close of the Business
The Insider Threat

Fig. 7. Insider Attack

### B. Cloud Malware Injection Attacks

In this type of attack, a manipulated copy of cloud consumer service occurrence is installed by the attackers into the cloud environment. This will generally permit them to load needs of victim service in their instances. The cloud infrastructure layer is attacked here and it also provides the attackers secret data, private data, etc [4][9].

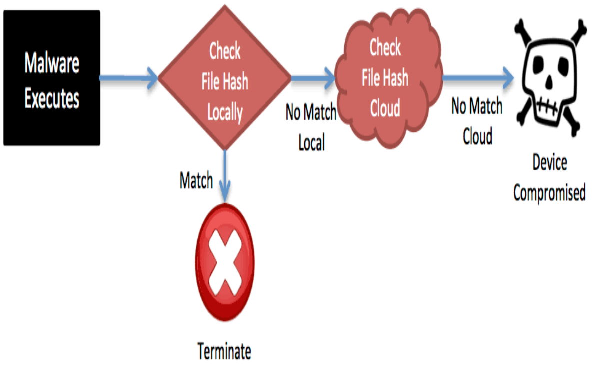


Fig. 8. Cloud Malware Injection Attacks

### C. Account & Service Hijacking Attacks

In the IT world, this type of attack is not new but still is a peak threat. The attackers misuse the software vulnerabilities and frequently send links to the users such as through messages, emails which can help them receive sensitive data such as passwords, credentials of the users. If the attacker gets access to consumer private data, he can listen to consumer activities and use the power of consumer status to begin other various attacks. In cloud case, this type of attack is done through any social engineering techniques or by illegal use of cloud [4][12].

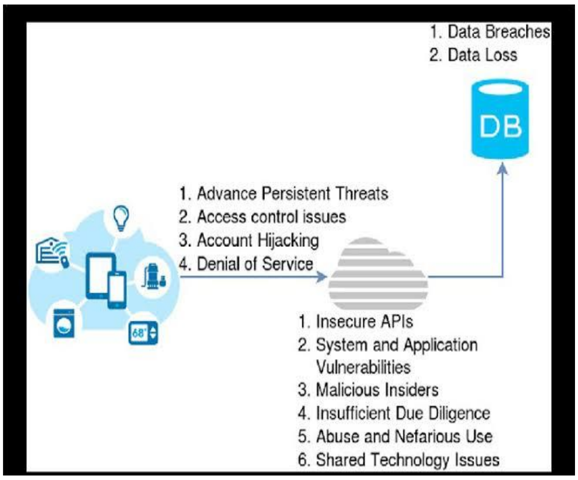

1. Data Breaches
2. Data Loss
DB
1. Advance Persistent Threats
2. Access control issues
3. Account Hijacking
4. Denial of Service
1. Insecure APIs
2. System and Application Vulnerabilities
3. Malicious Insiders
4. Insufficient Due Diligence
5. Abuse and Nefarious Use
6. Shared Technology Issues

**Fig. 9. Service Hijacking Attack**

### D. Cryptographic Attacks

To cloud services adoption, data privacy and reliability has become a major and important concern. The effective and best way to overcome the threats is by using cloud computing security which works on cryptographic techniques. Integrity and confidentiality is ensured by cryptographic techniques when stored and transmitted. However, in cloud case, the private key can be accessed only by the consumer. So, even the cloud provider cannot access the data.

Moreover, high level of data integrity and confidentiality is ensured by the cryptographic techniques. Unauthorized data is being threatened by different cipher attack techniques. Amongst the above attacks: Differential, Algebraic, Linear and Error Directive based Cryptanalysis [10], and each and every one of it has definite characteristics according to cryptosystems. The main agenda of this attack is to alter the data and we know that everything is available and can be used over internet which is provided by the cloud. Therefore, this atmosphere is easier to attack compared to other attacks. This attack mainly threatens three levels: data dispatched over internet, the cloud consumers and data stored in the cloud environment.

### E. Cloud consumer

Even if the consumer has the private key, the attackers use various methods and steal data from consumer's device by attacking consumer private key. Generally, the encryption key is given by the cloud provider; hence, a spiteful system administrator can insert software malware into the system and steal the data of the consumer by using private key.

### F. Data over the internet

We know that cloud provides data widely over the internet; hence, there are many threats for the data which is transmitted between cloud service provider and cloud consumer. The attackers can interrupt and recover the decryption key and also they can manipulate the data and affect the data cohesion.

### G. Data stored in cloud

Data is initially encrypted as per consumer's choice and is then sent to the cloud. Encryption keys are used to store the encrypted data alongside the public keys by the encryption keys for the long time in cloud environment. Hence, the attackers can access the private keys and private data during this long duration of time and this may even effect on the data integrity. The brute force attack [10] among all cryptographic attack tries all possible private keys to decrypt data.

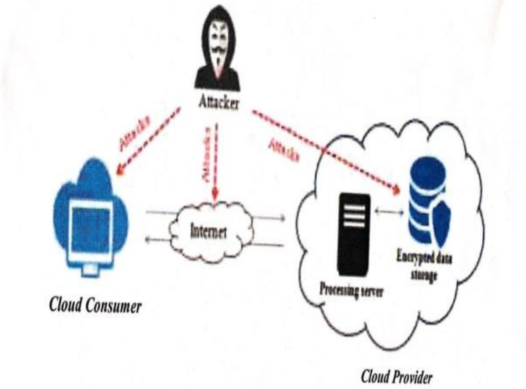


**Fig. 10. Attacks on a Cloud**

Some of the security threats and attacks against cloud computing are as given in the table I.

**Table - I: Attacks and Threats against Cloud Computing**

| SECURITY THREATS AND ATTACKS | CPSM LAYER |
|---|---|
| Insider attacks | CISL,PESL |
| Cloud malware injection attacks | CISL |
| Cryptographic attacks | DL,NSL |
| Account and Service Hijacking attacks | CISL,NSL,ACPLM |

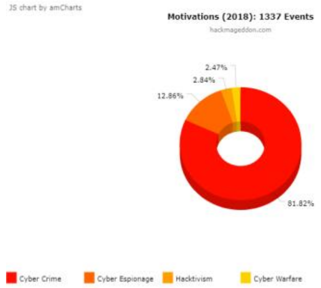


**Fig. 11. Pie-Graph showcasing Different Cyber Attacks**

The pie graph in the figure 11 shows the percentages of various clouds attacks such as cyber attacks taken place in 2018 by recording 1337 events. The highest record is set by Cyber crime which is 81.82%, second highest being Cyber espionage which has recorded 12.86%, third is Hacktivism which is 2.84%, the last being Cyber warfare which is 2.47%.

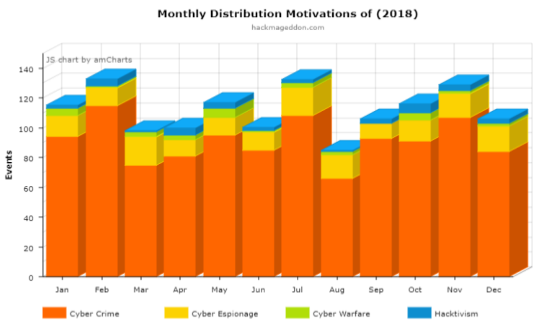


**Fig. 12. Motivation distribution graph for year 2018**

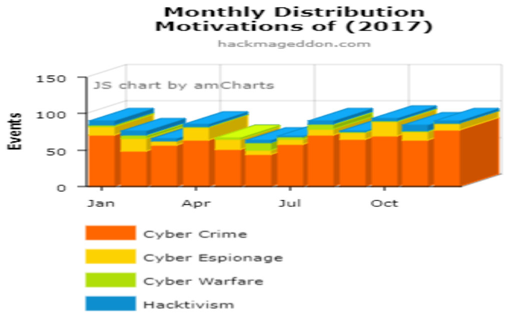


**Fig. 13. Motivation distribution graph for year 2017**

As we compare both figure 12 and figure 13, we could notice that the cloud threats have remarkably increased from 2017 to 2018.

## VIII. RELATED WORKS

Many researchers have been done and are going on to identify cloud privacy and security issues. In reference [7], authors showed their work on vulnerabilities concerned with virtualization infrastructure, cloud security issues, data security, software platform, etc. The authors classified cloud security issues into 4 types.

First being the Cloud Infrastructure, hosted code and platform. This is linked to storage, virtualization and networking passivity.

The second is the Data Category, which is about Data Lock, Data Integrity, etc.

The third being access category and it deals with Authorization and Authentication.

Finally, the last one is Compliance Category, which is mainly about Data Location, Security Audit, etc.

In [4], Kjalil et al. based on work and other connected works [7] to present survey regarding Cloud privacy and Cloud security. They also provided comparative analysis of countermeasures.

Moreover, in [4], the authors categorized cloud relevant attacks into 9 divisions: cloud malware injection, denial of service, targeted shared memory, VM rollback attack, Steganography, theft of service, phishing, VM side channels and botnets.

In [5], CSMIC developed SMI which helps the organizations in measuring cloud based business services. SMI is classified into 7 categories: privacy, performance, accountability, agility, usability, security, assurance and financial and every category is distinct by more than 3 attributes.

According to reference [4], auditing, SLA, service provider and other stakeholders together include to form security standard category. Re-availability of data with privacy and integrity is difficult to ensure with respect to these attacks. Hence, providers must understand the difference between those which threaten data security and which menace data availability. This will allow adopting countermeasures required in protection of data and availability of services in cloud environment.

## IX. COUNTERMEASURES

Till now, we have discussed about the CSPM model and security and privacy threats. Now, we are going to concentrate on security techniques and methods which can be acquired for access control and privilege management layers of CSPM.

### A. Later containing Data

The major obstacle in cloud services adoption is seeing or accessing private data. Cryptographic techniques are helpful techniques in this type of atmosphere and they are classified into 2 types of cryptosystems [10].

- Symmetric key
- Homomorphic key

Data treatment and data confidentiality is ensured by these techniques. For the privacy of trade of secret keys (symmetric key cryptosystem), asymmetric key cryptosystems are generated. Coming to privacy storage service, data could be encrypted before passing it into the cloud atmosphere by means of symmetric key cryptosystems. Nevertheless, homomorphic encryption technique is the best way to ensure regarding data treatment and data confidentiality.

**Symmetric key cryptosystems**

Here, the data can be encrypted i.e can convert to inexplicable format. AES, RC4, Blowfish, etc are some examples of this type of cryptosystems and to decrypt and encrypt data they use the same key.

Symmetric key working is different to other cases when used in cloud environment. Generally, these kinds of cryptosystems are used to maintain confidentiality between sender and the recipient and in case of cloud, private key can only be accessed by the consumer when data is stored in cloud.

**Homomorphic Encryption technique**

Homomorphic Encryption [13] is one among the encryption technique where it gives the capability to do or change operations on the encrypted data to a third party and the third party does not know the private key. The operations generally depend on the properties of cryptosystems with which it can generate encrypted output. The outcome we get is similar as functioning unswervingly on raw data. Hence, to the cloud provider the outcome and data of a procedure remains private [6].

### B. Access Control and Privilege Management Layer

Privilege management and access control are processes and rules adopted by cloud providers to make sure only consumers with certain privileges can access, vary the information.

Many different models like ABE, key policy aspect based encryption, etc have been suggested by many researchers which are useful to access control and provider security. But, many of the proposed models are modified forms of ABE. Based on attributes, decryption and encryption of data will be done by the users [2]. Secret key of ciphers and user are reliant on user characteristics. A cipher text decryption is possible only when cipher text attributes matches attributes of user key. To access information, concept of keys is used by maximum access control techniques.

## X. CONCLUSION

In this paper, CSPM model has been proposed which is a layered model and can help cloud consumers and providers with security and privacy issues. We have also discussed security threats and some countermeasures to those threats. As we know, cloud is highly dynamic and widely distributed and also easy to attack. To work effectively in cloud environment, the countermeasures should be improved so that security and privacy threats will be minimized.

## REFERENCES

1. P. Mell, T. Grance, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, U. S. Department of Commerce, September 2011.
2. A. RajaniKanth, M. Lakshmi, "A Survey on Access Control Models in Cloud Computing," Emerging ICT for Bridging the Future. Advances in Intelligent Systems and Computing, Vol. 337. Springer International Publishing, Switzerland, pp. 653-664, 2015.
3. M. Kandias, N. Virvilis, D. Gritzalis, 'The Insider Threat in Cloud Computing," Critical Information Infrastructure Security. Lecture Notes in Computer Science, Vol. 6983. Springer-Verlag, Berlin Heidelberg, pp. 93-103,2013.
4. Issa M. Khalil, A. Khreishah, M. Azeem, "Cloud Computing Security: A Survey," Computers, Vol, 3, pp. 1-35,2014.
5. The Cloud Services Measurement Initiative Consortium (CSMIC): Service Measurement Index Framework Version 2.1. Carnegie Mellon University Silicon Valley Moflett Field, CA USA, July 2014.
6. K. EL MAKKAOUI, A. EZZATI, A. BENI-HSSANE, C. MOTAMED, "Data confidentiality in the word of c1oud," Journal of Theoretical and Applied Information Technology, Vo1.84. No.3, 2016.
7. S. Sengupta, V. Kaulgud, V.S. Sharma, "Cloud computing security Trends and research directions," In Proceedings of the 2011 IEEE World Congress on Services, Washington, DC, USA, pp.524-531, 2011.
8. S. Kamara, K. Lauter, "Cryptographic Cloud Storage," Financial Cryptography and Data Security. Lecture Notes in Computer Science, Vol. 6054. Springer-Verlag, Berlin Heidelberg, pp. 136-149,2010.
9. N. Gruschka, M. Jensen, "Attack surfaces: A taxonomy for attacks on c10ud services," In Proceedings of the 2010 IEEE 3rd International Conference on Cloud Computing, Miami, FL, USA, pp. 276-279, 2010.
10. O. Cangea, G. Moise, "A New Approach of the Cryptographic Attacks," Digital Information and Communication Technology and Its Applications. Communications in Computer and Information Science, Vol. 166. Springer-Verlag, GmbH Berlin Heidelberg, pp.521-534, 2011.
11. K. HyunHo, B. Ndibanje, L. Hoon-Jae, C. YongJe, C. Dooho, "Side Channel Attacks on Cryptographic Module: EM and PA Attacks Accuracy Analysis," Information Science and Applications. Lecture Notes in Electrical Engineering, Vol. 339. Springer-Verlag, Berlin Heidelberg, pp. 509-516,2015.
12. CLOUD SECURITY ALLIANCE: The Notorious Nine: Cloud Computing Top Threats m 2013. https://c1oudsecurityalliance.org/group/top-threats.
13. M. Ogburn, C. Turner, P. Dahal, "Homomorphic Encryption," Procedia Computer Science 20, Elsevier, pp. 502 - 509, 2013.
14. Tian Xia1, Hironori Washizaki2, "Cloud Security and Privacy Metamodel Metamodel for Security and Privacy Knowledge in Cloud Services," (MODELSWARD 2018), pages 379-386, ISBN: 978-989-758-283-7.

## AUTHORS PROFILE

**Ms. Gouni Ritthiika Reddy** is currently pursuing B.Tech Degree program in Computer Science & Engineering in Sreenidhi Institute of Science and Technology, Affiliated to Jawaharlal Nehru Technical University Hyderabad, Telangana, India. Her main research work focuses on Medical Image Processing, Machine Learning, Cloud Computing and Neural Networks

**Mr. Devevarapu Sreenivasarao**, currently working as an Assistant Professor in the department of CSE in Sreenidhi Institute of Science and Technology since 2014. He did Master of Technology from JNT University Hyderabad, India in year 2012. He is a research scholar in Annamalai University which was located in Chidambaram, Tamilnadu, India He has published more than 15 research papers in various peer reputed international journals..His main research work focuses on Medical Image Processing, Machine Learning.

**Mr. Shaik Khasim Saheb** currently working as an assistant Professor in the department of CSE in Sreenidhi Institute of Science and Technology since 2014. He did masters from VIT University, Tamilnadu, India. 2014. He is a research scholar in Annamalai University which was located in Chidambaram, Tamilnadu, India. He has published more than 10 research papers in various peer reputed international journals. His main research work focuses on Medical Image Processing, Machine Learning.