COUNTERMEASURES FOR SECURITY ATTACKS IN CLOUD NETWORK TO AVOID DATA BREACHES: A REVIEW

[1]Shabnam Kaur, [2]Dr. Rajandra Gupta
[1]Research Scholar, Rabindranath Tagore University, Bhopal
[2]Associate Professor, Rabindranath Tagore University, Bhopal

ABSTRACT: Despite the fact that cloud computing brings preferences for the today's companies, there are numerous defensive steps to be considered. Organizations need to actualize defensive measures to securely migrate and extend operations to the cloud, and putting resources into cloud security is significant to protection from threats. The Security and risk experts need to settle on the correct decision. Security and risk (S&R) professionals are struggling to prevent data breaches, threats from noxious insiders, and misrepresentation. This paper attempted to give solutions for secure user behavior ,mean to give S&R professionals to detect suspicious action and to stop it before it makes enduring mischief the business. Privilege Identity Management is basic for defeating threats and minimizing data breaches.

Keywords: Threats, Data Breaches, Security and risk (S&R), Privilege Identity Management (PIM)

I. INTRODUCTION

A breach is characterized as an event in which a person's name, medical record, a monetary record or debit card is conceivably put in risk—either in electronic or paper format. There is a steady increase in successful cyber attacks. Palo Alto Networks, Gartner Magic Quadrant Firewall Leader for Sixth Year, investigates the enterprise security for endpoints, which are still in the hands of antivirus solutions in numerous spots. Palo Alto Networks notes that threats and attackers have evolved, but many security solutions have not. The most popular security techniques include SSL (Secure Socket Layer) Encryption, Intrusion Detection System; Multi Tenancy based Access Control, etc. Goal of this paper is to analyze and evaluate the most important security techniques for data protection in Network cloud.

II. LITERATURE REVIEW

Kire Jakimoski [1] focuses on the survey of the top security concerns related to cloud computing. For each of these security threats they describe, how it can be used to exploit cloud components and its effect on cloud entities such as providers and users and the security solutions that must be taken to prevent these threats. These solutions include the security techniques from existing literature as well as the best security practices that must be followed by cloud administrators but there should be some strategies to mitigate security issues from user sides. [4]Compared three cloud service models. Clouds provide a powerful computing platform that enables individuals and organizations to perform variety levels of tasks such as: use of online storage space, adoption of business applications, development of customized computer software, and creation of a “realistic” network environment.[14][16]. If security is not robust and consistent, the flexibility and advantages that Network cloud has to offer will have little credibility. Kire Jakimoski[15] recommended security techniques for data protection to improved security in Network cloud. The current threats are more sophisticated, more automated, cheaper to run and can take various forms. The attackers act in a larger style and at a faster pace. Many companies are not prepared for this. All this has escalated in recent years, according to Palo Alto Networks, while many security tools, solutions, and platforms have maintained the same practices as decades ago.

Table-1: Number of Breaches incidents By Type

Type	Incidents	Percentage
Identity Theft	880	53%
Nuisance	66	4%
Existential Data	175	10%
Account Access	182	11%
Financial Access	370	22%

Source: Breach Level Index

Table-2: Number of Breaches incidents By Source

Source	Incidents	Percentage
Malicious Outsider	964	58%
State Sponsored	33	2%
Hacktivist	36	2%
Malicious Insider	238	14%
Accidental Loss	398	24%

The Breach Level Index (BLI) is a global database that tracks data breaches globally and measures their severity based on multiple dimensions, including the type of data and the number of records compromised, the source of the breach, and whether or not the data was encrypted. According to the Breach Level Index, more than 3.6 billion data records have been exposed since 2013 when the index began benchmarking publicly disclosed data breaches. In 2015, malicious outsiders were the leading source of these breaches, accounting for 964, or 58% of breaches and 38% of compromised records, while identity theft remained the primary type of breach, accounting for 53% of data breaches and 40% of all compromised records.

Table-3: Organizations facing Data Breaching

Organization Breached	Record Breached	Date of Breach	Type of Breach	Source of Breach	Location	Industry	Risk Score
Facebook	2,200,000,000	04/04/18	Identity Theft	Malicious Outsider	United States	Social Media	**10.0**
Twitter	336,000,000	05/03/18	Financial Access	Accidental Loss	United States	Social Media	**9.0**
Exactis	340,000,000	06/01/18	Identity Theft	Accidental Loss	United States	Other	**9.1**
Adidas	2,000,000	06/26/18	Identity Theft	Malicious Outsider	United States	Retail	**7.5**
Ministry of defence/Ex-Servicemen Contributory Health Scheme (ECHS)	5,000,000	03/21/18	Account Access	Malicious Insider	India	Government	**7.5**
Facebook	3,000,000	04/07/18	Identity Theft	Hacktivist	United States	Social Media	**7.4**
BSNL	47,000	03/02/18	Account Access	Malicious Outsider	India	Education	**5.6**
NEET/NBE/ Union Ministry of Health and Family Welfare	22,250	01/25/18	Identity Theft	Malicious Insider	India	Education	**5.4**

Source: breachlevelindex.com

III. METHODOLOGY USED

A lot of business executives are familiar with the benefits of cloud computing that are been offered over a traditional in house IT departments. But as the popularity of this new alternative expands, questions concerning to its security are being raised. Is cloud computing as safe as having your data network in house? Questions are asked from the respondents who are working on internet protocol. They are using Cloud computing as a new supplement, consumption, and delivery model for IT services based on Internet protocols. Direct mailing procedure is used to send the prepared questionnaire to experts and few of responses are taken from direct interaction with experts currently having industrial experience in Network cloud.

IV.SURVEY RESULTS

The statistic results shows the risks of cloud computing for enterprises worldwide, according to survey conducted by RightScale. In Figure-1, 27% of respondents indicated that a lack of resources or expertise for cloud computing was a risk of cloud adoption for their enterprise.

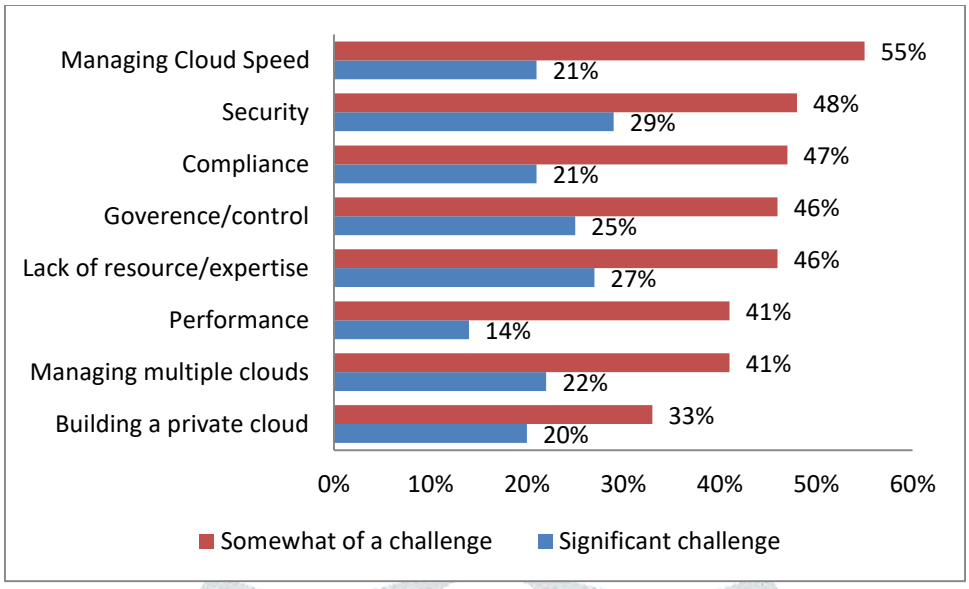
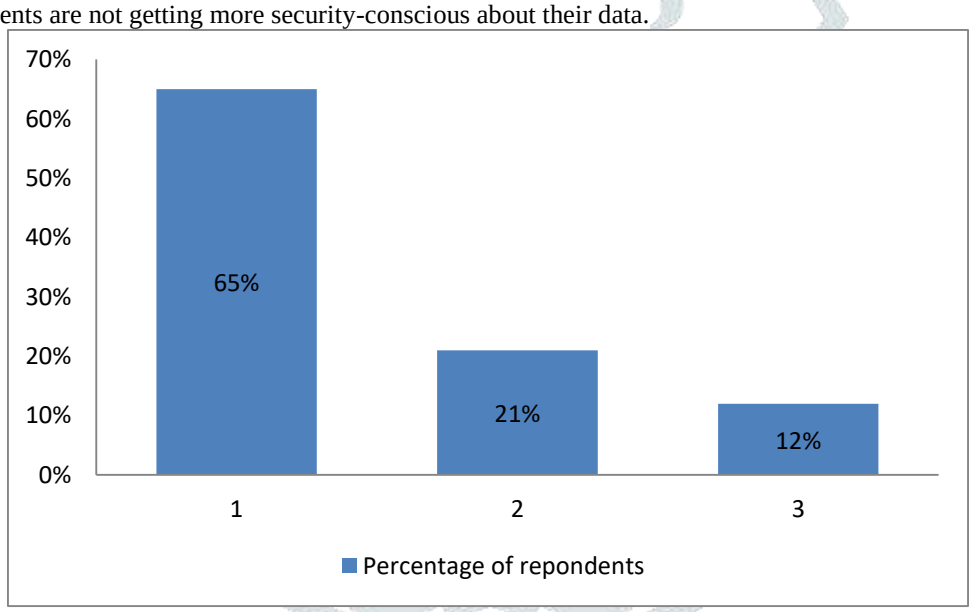


Figure 1 : Challenges of Cloud Computing worldwide

In Figure-2, the survey shows the percentage of respondents who are getting more security-conscious about their data. 12% of the respondents are not getting more security-conscious about their data.



Source: Identity Theft Resource Center(ITRC)

Figure 2 : Getting more security-conscious about their data.

The chart in figure-3 shows exactly how the last few years have seen a surge in hacking attacks targeting sensitive information. The number of significant breaches at U.S. businesses, government agencies, and other organizations topped 1,300 last year, versus fewer than 200 in 2005. It is the opinion of the ITRC that the criminal populace is stealing more information from organizations, and data breaches are as a rule all the more frequently publicized," the nonprofit says on its site, with more organizations revealing breaches due to laws or public pressure. But at the same time it's difficult to decide if there are more security breaches now than any time in recent memory, as per the ITRC.

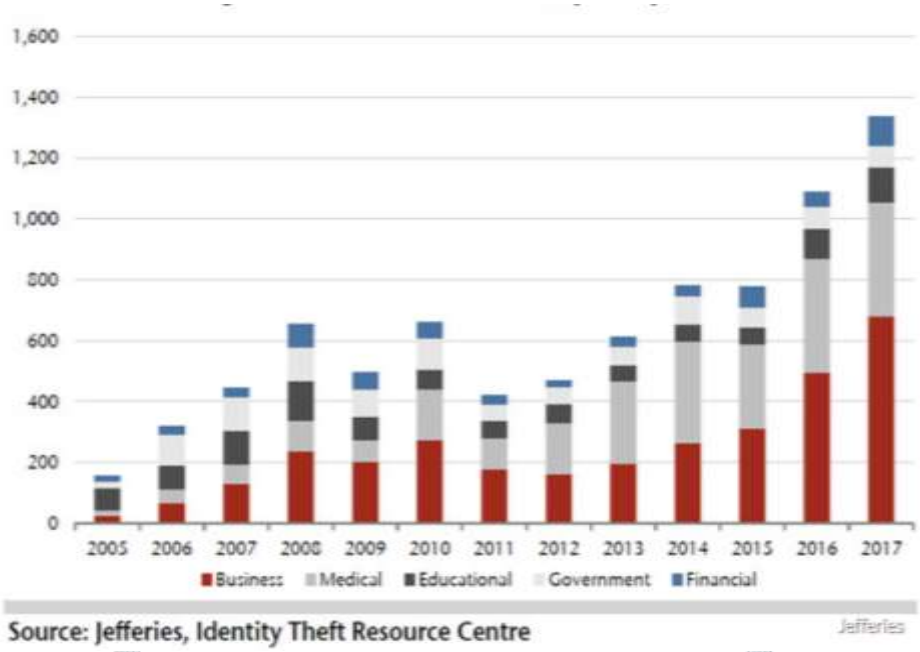


Figure 3 : Increasing number of data breaches(by entity)

The Privacy Rights Clearinghouse maintains a public database of breaches across industries. The total number of records breached is 907,453,926 since they started record keeping in 2005. Results for two time periods, 2010 and 2016-2017 to try to see any trends in the data. The results are shown in the chart.

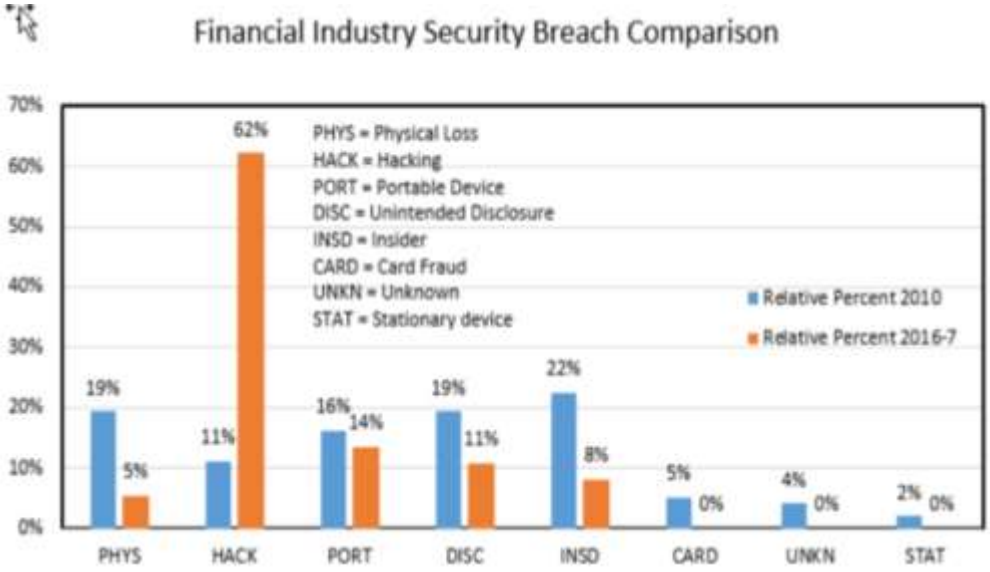


Figure 4: Financial Industries Security Breaches Comparison

It's pretty obvious that hacking attacks have been increasing and that financial institutions' defenses in this area need to improve. This type of thought process should be used in the risk management process. It is needed to look at not only privacy breaches but also data integrity breaches (wire fraud) and denial of service attacks.

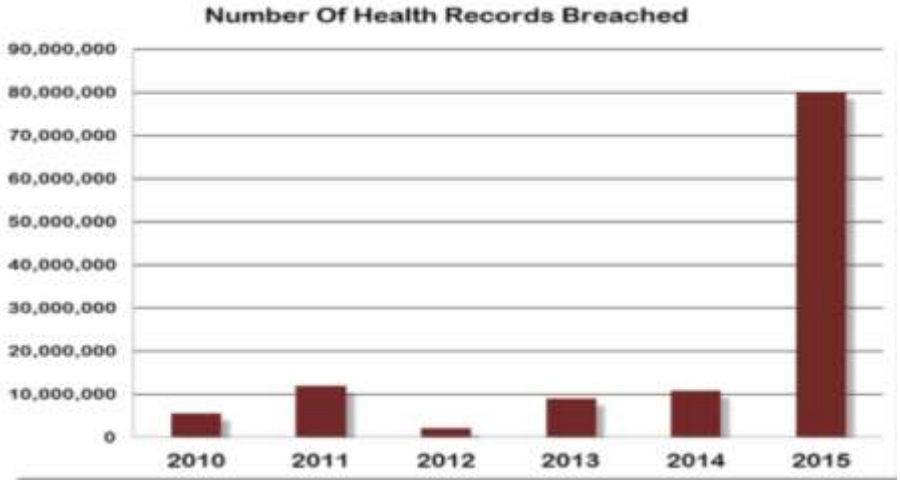


Figure 5 : Number of Health Records Breached

In 2015, data breaches in Healthcare totaled more than 112 million records, as per an article as of late distributed by Forbes. As per the Office of Civil Rights (OCR), which distributed data breaches as answered to them and required by HIPPA, there were 253 healthcare data breaches that influenced somewhere around 500 people, with a consolidated loss of more than 112 million records in 2015.

4.1 Cloud Security Statistics

1. Only **7%** of businesses have good visibility of all critical data. **58%** say they only have slight control[8]
2. Vulnerabilities: **24%** of organizations have hosts missing high-severity patches in public cloud.[9]
3. **80%** of security breaches involve privileged credentials.[10]
4. **49%** of databases are not encrypted.[9]
5. **73%** of security professionals who report that their organization has not implemented a privileged account security solution for DevOps [11]
6. Worldwide public cloud services market is projected to grow over 21% in 2018, totaling $186.4 billion (an increase of over $33 billion in one year).
7. Through 2022, at least **95%** of cloud security failures are predicted to be the customer's fault.[12]
8. An average of **51%** of organizations publicly exposed at least one cloud storage service.[9]
9. When asked about adopting an enterprise cloud computing platform, **66%** of IT professionals say security is their greatest concern.[13]
10. Only **12%** of global IT organizations understand how GDPR will affect their cloud services.[13]
11. **25%** of organizations have cryptojacking activity within their environments.[9]
12. **84%** of organizations say traditional security solutions don't work in cloud environments.[13]
13. Public cloud account compromises are fueling new attack vectors, causing **27%** of organizations to have users whose accounts are potentially compromised.[9]

V. PROTECTION AGAINST DEBILITATING DATA BREACHES

5.1 Conducting Risk Assessment

Conducting a yearly security risk analysis is a prerequisite of the Security Rule, so it is best to design it ahead of time and make room in your financial plan for it. There are countless changes that occur throughout a year, including "new system deployments, IT infrastructure enhancements authoritative rebuilding and representative turnover. At the point when the majority of the progressions are thought of it as, leaves a great deal of space for new vulnerabilities to emerge. Since IT circumstances fluctuate so rapidly, it's critical to schedule regular risk analyses.

5.2 Implement Data and Hardware Encryption

It's best to insist on encryption of data and hardware devices, especially when it comes to portable devices. Data encryption is considered a key way of preventing data breaches. When encryption is referred, it is essentially referring to the translation of data into a secret code that requires a username and password to gain access to the decrypted data. According to fourth annual Breach Report, encrypting laptops and other portable devices has been their top recommendation every single year. From 2009 to the present, the loss or theft of unencrypted portable devices have made up over a third of all large breach incidents and impacted over 50 percent of record put at risk.

While there are certainly hurdles to defeat with regards to encryption, including budgetary constraints, client preparing requirements and employee resistance (to give some examples), the expense of execution could not hope to compare to the pain that accompanies a noteworthy shoreline episode because of the loss of an encrypted device full of private information.

Some of the security algorithms are :

- RSA algorithm for secured communication

- AES for Secured file encryption
- MD5 hashing for cover the tables from user
- One time password for authentication

5.3 Conduct Frequent Vulnerability and Penetration Assessments

Vulnerability management is basic to cloud security and system security.

While dangers from hackers and different noxious outcasts it not the main source of data breaches, they are anticipated to become a much larger threat in years to come. Hackers can possibly cause significant issues for enterprises. The purpose behind this is for instance close to personal records are high esteem focuses for cybercriminals, as they can be exploited for identity theft, fraud, stolen prescriptions and hazardous scams, what's more, numerous types of providers process and store credit card information.

5.4 Security by Design and Architecture

Security by design, or then again secure by design, implies that the software has been designed starting from the earliest stage to be secure. Security is considered as a primary component. It is identified with access control and Authorization. Some of the techniques in this approach include:

Least Privileges : Privileges should be given for each part of the system .

Automated theorem proving : to prove the correctness of crucial software sub-systems.

Code reviews and Unit testing approaches *:* to make modules more secure where formal correctness proofs are not possible.

The security architecture varies dependent on the kind of cloud model. IaaS infrastructure gives the storage and networking components to cloud networking. It depends vigorously on application programming interfaces (APIs) to enable enterprises to oversee and collaborate with the cloud. IaaS cloud computing service models require these extra security highlights:

•Virtual web application firewalls and network-based firewalls

•Virtual routers

•Intrusion Detection Systems and Intrusion Prevention Systems (IDS/IPS)

•Network division

Cloud Access Security Brokers (*CASB)* play a central role in discovering security issues within a SaaS cloud service model as it logs, audits, provides access control, and oftentimes includes encryption capabilities. Security features for the SaaS cloud environment include:

- Logging
- IP restrictions
- API gateways

The Cloud Service Provider secures a majority of a PaaS cloud service model. However, the security of applications rests with the enterprise. The essential components to secure the PaaS cloud include:

- Logging
- IP restrictions
- API gateways
- CAS

5.5 Educating your end user

The end-user is widely recognized as the weakest link in the security chain and it is estimated that more than 90% of security incidents and breaches involve some kind of human error. Among the most commonly recorded forms of errors and misjudgment are poor password management, the inability to recognize misleading URLs and to identify fake websites and dangerous email attachments.

5.6 Response to breaches

Responding forcefully to endeavored security breaches is frequently exceptionally troublesome for a variety of reasons:

Identifying attackers is difficult, as they are frequently in a different jurisdiction to the systems they endeavor to rupture, and work through intermediaries, brief mysterious dial-up records, remote associations, and other anonymising procedures which make back following troublesome and are regularly situated in one more locale. On the off chance that they successfully breach security, they are regularly ready to delete logs to cover their tracks.

5.7 Data Protection and Recovery

Data stealing problem is the most conventional approach to break a user account in cloud computing environments . The account password is stolen by attackers. Then the attacker cracks the confidential information the cloud computing environments. In sometimes they crash the system information's. The service providers and cloud users are affected by those kinds of problems. It is very important each system that is using cloud computing to has automatic back up procedure at least once a week, and for systems that store sensitive information even more frequently than once a week. The overall backup procedure should even include the operating system, application software and data on the machine. Multiple backups over time could be also implemented and policies of backup should be in compliance with any official or regulatory requirements.

VI. PIM Is Critical For Defeating Threats And Minimizing Data Breaches

Previously, regulatory compliance and administrative efficiency were the key drivers for implementing privileged identity management (PIM) solutions[1].However, security and risk (S&R) leaders today rightly view PIM solutions as key components of their multilayered defenses against cyber threats, alongside elements like network security, security analytics (SA), security user behavior analytics (SUBA), identity and access management, cloud security solutions, and endpoint security solutions:

Cyber threat includes utilization of privileged credentials. Forrester estimates that 80% of security breaches include advantaged qualifications. S&R pros can't dispose of shared and business credentials, so should oversee them. In a perfect world, there should not be shared passwords or recycled/shared functional accounts.

For cloud adoption there should be a new admin types and access channels. Adoption of infrastructure-asa-service (IaaS) (from providers like AWS, Azure, and Rackspace) and software-as-a-service (SaaS) (like Salesforce and Office 365), public cloud applications, private cloud, and outsourcing creates a new kind of administrator (or privileged user): one who is an employee of f the public or private cloud provider (AWS, Azure, SoftLayer, etc.) and interacts with your workloads on their behalf. These users may not have VPN access to your environment and often require very controlled, limited, and closely monitored access to your workloads.

PIM demands an incorporated methodology from admin's entry point to the objective system. Security teams progressively find that they can't keep up homegrown or potentially point answers for overseeing favored access without using restrictive measures of exertion. Beyond multifactor authentication (MFA) and security assertion markup language (SAML) similarity, a PIM arrangement needs have the capacity to complete four things: 1) give its own, online channel for access; 2) give its own, carefully designed secret key safe (certification stockpiling); 3) bring forth, screen, and catch favored Windows and Linux sessions (privileged session monitoring, or PSM); and 4) control benefit acceleration on the endpoint.

VII. CONCLUSION

The main goal of this paper is to analyze and evaluate the security techniques for data protection in the cloud computing. Conducting internal risk assessment and planning, and most importantly employ the right security technologies to help ensure that if a breach will to occur, high value and most sensitive data would not be compromised. For this purpose, the most important security techniques are analyzed and evaluated for data protection that are already accepted from the cloud computing providers. This paper recommended important security measures relating to data protection in the cloud that must be taken into account.

VIII. REFFERENCES

[1] Kire Jakimoski , Security Techniques for Data Protection in Network cloud , 2016, pp.49-56 http://dx.doi.org/10.14257/ijgdc, 2016
[2] Andras Cser, Joseph Blankenship, Merritt Maxim, Nick Hayes ,Market Overview: Security User Behavior Analytics (SUBA), 2016
[3] Te-Shun Chou "Security Threats on Cloud Computing Vulnerabilities, International Journal of Computer Science & Information Technology (IJCSIT) , June 2013
[4] Collaboration and Internet Computing (CIC), 2016 IEEE 2nd International Conference on Date of Conference: 1-3 Nov. 2016 Date Added to IEEE Xplore,2017
[5] Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on Date of Conference: 16-18 March 2016 Date Added to IEEE Xplore,2016
[6] Santosh Khamitkar, Yaser Fuad Al-Dubai, Parag Bhalchandra, Pawan Wasnik, Kerberos Authentication with Cloud Computing Access Control, International Journal of Grid and Distributed Computing,2016
[7] S. A. Alhumrani1 and Jayaprakash Kar," Cryptographic Protocols for Secure Cloud Computing",2016
[8] Saheli Sen Gupta, Lesser data visibility leads to higher cybersecurity risks: Study,2017
[9] RedLock, Cloud Security Trends - Anniversary Edition - May 2018
[10] Andras Cser, The Forrester Wave™: Privileged Identity Management, 2016
[11] CyberArk Global Advanced Threat Landscape Report, Focus on DevOps
[12] Kasey Panetta, Recommendations for developing a cloud computing strategy and predictions for the future of cloud security.
[13] Louis Columbus, Asokan Ashok, Crowd Research Partners, Cloud Security Report 2018
[14] Monjur Ahmed and Mohammad Ashraf Hossain ,Cloud Computing and Security issues in the Cloud International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, 2014
[15] Yunchuan Sun, Junsheng Zhang, Yongping Xiong, Guangyu Zhu,Data Security and Privacy in Cloud Computing, 2014
[16] Cloud Computing and Security issues in the Cloud International Journal of Network Security & Its Applications Vol.6, No.1, January 2014, Monjur
[17] Mather T, Kumaraswamy S, Latif S ," Cloud Security and Privacy". O'Reilly Media, Inc., Sebastopol, CA,2009.