\documentclass[a4paper,twoside]{article}

\usepackage{amsfonts,amssymb,amsbsy,latexsym,amsmath,tabulary,graphicx,xcolor}

\usepackage{amsmath,tabulary,graphicx,fancyhdr,times}

\usepackage[utf8]{inputenc}

\usepackage{caption}

\def\NormalBaseline{\def\baselinestretch{1.1}}

\usepackage{textcase}

\usepackage[T1]{fontenc}

\usepackage[margin=3cm,top=30mm,bottom=1in]{geometry}

\linespread{1.5} \date{}

%\def\floatpagefraction{0.8}

\captionsetup[figure]{labelsep=period,labelfont=bf,name=Figure}

\makeatletter\def\oupIndent{1pt}

\def\author#1{\gdef\@author{\hskip-\dimexpr(\tabcolsep)\hskip\oupIndent\parbox{\dimexpr\textwidth-\oupIndent}{\centering#1}}}

\def\title#1{\gdef\@title{\centering\bfseries\ifx\@articleType\@empty\else\@articleType\\\fi\selectfont #1}}

\fancypagestyle{headings}{\renewcommand{\headrulewidth}{.5pt}\renewcommand{\footrulewidth}{.5pt}\fancyhf{}\fancyhead[ER]{\journalTitle}\fancyhead[OL]{\AuthorName}\fancyfoot[OR]{\thepage}\fancyfoot[EL]{\thepage}}\pagestyle{headings}

\fancypagestyle{plain}{\renewcommand{\headrulewidth}{0pt}\renewcommand{\footrulewidth}{0pt}\fancyhf{}}

\let\@articleType\@empty \def\articletype#1{\gdef\@articleType{{\itshape#1}}}

\def\NormalBaseline{\def\baselinestretch{1.1}}

\usepackage[noindentafter,explicit]{titlesec}

\setcounter{secnumdepth}{5}

\titleformat{\section}[hang]{\NormalBaseline\centering\large\bfseries\boldmath\fontsize{11}{13.2}\selectfont\MakeTextUppercase}

{\large\thesection.\hspace{-6pt}}

{10pt}

{#1}

[]

\titleformat{\subsection}[hang]{\NormalBaseline\filright\bfseries\boldmath\fontsize{11}{13.2}\selectfont}

{\thesubsection\hspace{-6pt}}

{10pt}

{#1}

[]

\titleformat{\subsubsection}[hang]{\NormalBaseline\filright\bfseries\boldmath\fontsize{11}{13.2}\selectfont}

{\thesubsubsection\hspace{-6pt}}

{10pt}

{#1}

[]

\titleformat{\paragraph}[runin]{\NormalBaseline\filright\bfseries\boldmath\fontsize{11}{13.2}\selectfont}

{\theparagraph\hspace{-6pt}}

{10pt}

{#1}

[]

\titleformat{\subparagraph}[runin]{\NormalBaseline\filright}

{\thesubparagraph\hspace{-6pt}}

{10pt}

{#1}

[]

\titlespacing{\section}{0pt}{1.5\baselineskip}{.2\baselineskip}

\titlespacing{\subsection}{0pt}{1\baselineskip}{.2\baselineskip}

\titlespacing{\subsubsection}{0pt}{1.5\baselineskip}{.2\baselineskip}

\titlespacing{\paragraph}{0pt}{.5\baselineskip}{10pt}

\titlespacing{\subparagraph}{0pt}{.5\baselineskip}{10pt}

\makeatother

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

% Following additional macros are required to function some

% functions which are not available in the class used.

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

\usepackage{url,multirow,morefloats,floatflt,cancel,textcomp,tfrupee}

\usepackage{pifont}

\usepackage[nointegrals]{wasysym}

\urlstyle{rm}

\makeatletter

\AtBeginDocument{

\expandafter\ifx\csname eqalign\endcsname\relax

\def\eqalign#1{\null\vcenter{\def\\{\cr}\openup\jot\m@th

\ialign{\strut$\displaystyle{##}$\hfil&$\displaystyle{{}##}$\hfil

\crcr#1\crcr}}\,}

\fi

}

\let\lt=<

\let\gt=>

\def\processVert{\ifmmode|\else\textbar\fi}

\let\processvert\processVert

\@ifundefined{subparagraph}{

\def\subparagraph{\@startsection{paragraph}{5}{2\parindent}{0ex plus 0.1ex minus 0.1ex}%

{0ex}{\normalfont\small\itshape}}%

}{}

% These are now gobbled, so won't appear in the PDF.

\newcommand\role[1]{\unskip}

\newcommand\aucollab[1]{\unskip}

\@ifundefined{tsGraphicsScaleX}{\gdef\tsGraphicsScaleX{1}}{}

% To automatically resize figures to fit inside the text area

\def\checkGraphicsWidth{\ifdim\Gin@nat@width>\linewidth

\tsGraphicsScaleX\linewidth\else\Gin@nat@width\fi}

\let\ts@includegraphics\includegraphics

\def\inlinegraphic[#1]#2{{\edef\@tempa{#1}\edef\baseline@shift{\ifx\@tempa\@empty0\else#1\fi}\edef\tempZ{\the\numexpr(\numexpr(\baseline@shift\*\f@size/100))}\protect\raisebox{\tempZ pt}{\ts@includegraphics{#2}}}}

%\renewcommand{\includegraphics}[1]{\ts@includegraphics[width=\checkGraphicsWidth]{#1}}

\AtBeginDocument{\def\includegraphics{\@ifnextchar[{\ts@includegraphics}{\ts@includegraphics[width=\checkGraphicsWidth]}}}

\def\URL#1#2{\@ifundefined{href}{#2}{\href{#1}{#2}}}

%%For url break

\def\UrlOrds{\do\\*\do\-\do\~\do\'\do\"\do\-}%

\g@addto@macro{\UrlBreaks}{\UrlOrds}

\makeatother

\def\floatpagefraction{0.8}

\def\dblfloatpagefraction{0.8}

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

\usepackage[numbers]{natbib}

\begin{document}

\def\authorCount{4}

\def\affCount{4}

\def\journalTitle{Survey On Methods/Mechanisms For Providing Data Security In Cloud Environment}

\def\AuthorName{Lekshmi}

\title{SURVEY REPORT}

\author{TOPIC: \textit{SURVEY ON METHODS/MECHANISMS FOR PROVIDING\\

DATA SECURITY IN CLOUD ENVIRONMENT}\vspace\*{10cm}\\\hspace\*{10cm}\textit{SUBMITTED BY}\\\raggedleft\bfseries{LEKSHMI BABU\\ROLL NO 10\\M1 NE}}

\maketitle

\newpage

\section\*{Introduction}

Cloud Computing is a growing field in the area of computing. It is a way to maximize the utilization and computing capabilities without spending a lot to buy a new infrastructure. Cloud computing services are having various features such as liability, versatility, dependability, adaptability, profitability and element property. The resources in the cloud can be scaled in any direction, by the prerequisites of the client, to build the assignment execution. Cloud computing is a distributed network computing technology cite{1}.It conveys infrastructure, programming and application as administrations to the client through the internet. These amenities are delivered by using virtualization technique of the data center. Data center is a pool of servers which accommodate all the applications of the clients of cloud. The clients and undertakings can utilize these server farms to store and process their information in outsider, by the utilization of cloud computing. Cloud computing relies on sharing of resources to achieve lucidity and economy of scale. Users can get faster access to their data on cloud due to this immense storage mechanism. The service availability issues are monitored by the service provider. As per NIST Cloud computing is characterized as "an approach to empower suitable, on-request network access to a mutual group of computing resources that can be promptly provisioned and released with least administration effort”.One of the examples for such a noble innovative technology is the popular social networking site called Face book. Users need only an internet connection to access the site through their login credentials. Users can use Face book to share photos, images and multimedia contents. All these data can be accessed by the users anytime anywhere if they are having internet connection because information is put away in remote computer framework rather than neighborhood computer framework using cloud computing.

Cloud computing exists when several computers are accessing the services from the internet. The cloud computing systems are fault tolerant. Hence they provide dependable services to the client. Cloud computing offers different services to the users such as hardware, software, information get to and capacity. The clients can get to these services from the cloud without having any data about the physical area and arrangement of the framework which offers the services. In view of the utilization necessity of the clients, Cloud is categorized into three models. \\

\subsection\*{Private Cloud:} The cloud infrastructure is developed for the own purpose of the organization. The specific group of workers can access this cloud. Public users cannot access this

cloud.\\

\subsection\*{Public Cloud:} The cloud can be used by the general public. Any user at anytime from anywhere can access the services from public cloud. The users are charged based on the utilization level of the cloud services.\\

\subsection\*{Hybrid Cloud:} The mix of private and public cloud is called hybrid cloud. This is built up when the private cloud needs a few amenities from the public cloud. Cloud computing environment offers three types of service models. Users can select any one of these three services based on their need. The users can use these services based on pay for use model. The users are charged based on their usage volume.

The three Service Models offered by cloud computing are:\\

\subsection\*{Software as a Service (SaaS):} The different applications running on a cloud can be approached to by the client through a web program. Face book, Whatsapp, Gmail etc. are such services.\\

\subsection\*{Platform as a Service (PaaS):} The level above SaaS is PaaS. The client is permitted to get to the operating framework to deploy the developed applications on the cloud. The required resources can be provided to the users through this model. It is not essential for the user to install and maintain the required

software in his/local system. So the cost required for developing the application through cloud computing

environment is very less. Example: Google App Engine. \\

\subsection\*{Infrastructure as a Service (IaaS):} The required infrastructure can be given to the clients through this model. A portion of the infrastructure assets are hard ware equipment, storage and bandwidth. For example if a user wants to have five computer systems with some specific configurations to develop an application, he/she can access or use those computers through this service model from the cloud service provider without spending a lot to buy new computers. Example: Amazon EC2 cloud.

\section\*{RELATED WORK}

Security is a primary concern when it comes to adoption of cloud computing as a primary source for data storage. In recent years, work has been dedicated to develop security framework and mechanisms to protect user data. Ida Madieha et al layout the issues and difficulties from the purposes of legitimate structure that Malaysia ought to expect and address in keeping up and maintaining its national critical information infrastructure(CII). They likewise have first take a gander at the issue of information breach on the planet and analyze how as the innovation turns out to be more predominant, the digital world turns out to be more defenseless against information breaks. Attached to that is the thought of critical information infrastructure. The potential cost of data misfortune to organizations and society is expanding yearly. Along these lines, there is a requirement for a monetary model to compute the costs identified with data breach occurrences with solid prescient abilities. Abdullah M. Algarni et al analyze the present condition of existing methodologies, which frequently differ as far as strategies and results. There is a need to accommodate all the profitable methodologies and expand on them. This would permit us to make a more total single approach that could dependably survey the different data breach cost segments. Chandramohan.D et al focus on privacy preserving technique. They have perceived the week benefit holding of cloud suppliers in fulfilling, and guarding clients' mystery and failed to have an all inclusive service level understanding. To encounter the privacy issue, the authors have proposed a privacy reserving algorithm cite{2}. Nina Pearl Doe and Suganya V ensure the corrective measures to protect the integrity of data as well as detecting and preventing possible risks thus ensuring data breaching is prevented. The system, however, concentrates mainly data breaches but there are more threats that cloud security faces. Mark L. Huson and Barbara Hewitt examine the effectiveness of regulation within several industries to determine whether increased regulation would result in a reduction in information compromises. David Kolevski and Katina Michael reviewed cloud computing data breaches using a socio-technical approach. The three major dimensions in the socio technical theory are- the social, the technical, and the environmental. The 7 key themes identified are: security, availability of data, privacy issues, trust, data flow, service level agreements, and regulation. Aryan TaheriMonfared and Martin GiljeJaatun review existing security monitoring mechanisms compared with new challenges which are caused by this new model. They highlight possible weaknesses in existing monitoring mechanisms, and propose approaches to mitigate them. A general analysis framework was proposed by Yoga chandran et al to compute risk related with data breaches by using pre-agreed Sec SLAs for various cloud providers. The framework contains a tree based structure to find potential attack which leads to data breaches in the cloud and a way to evaluate the use of possible mitigation approaches to reduce them. There have been initial attempts to model the security of cloud in terms of securing stakeholder’s computational space. Some recent attempts formally model the CBS (Cloud based systems) as modularized actor models, using rewriting &equation logic based modeling languages. Building on these works has presented a framework for building executable models of CBSs for security analyses and illustrate its validity showing how the recent security breaches and security solutions can be modeled and analyzed using this framework.\\

Although security is analyzed from different perspective, more attention is given for enhancing security and actual data breach issues are not considered. Our focus is to dig deep into the security issues of data breaches and their significances in data security.

\section\*{SECURITY ASPECTS}

Security is the major factor to be concentrated while adapting to the cloud. The users will maintain lot of personal and secured data in their personal computers. When they are using the cloud computing technology these data will be transferred from their computer to the cloud. Hence the cloud should have efficient security mechanisms to secure these data. The security issues in the cloud are - confidentiality, integrity, availability, and privacy. The security issues are as follows:\\

\subsection\*{Confidentiality:} Preventing the secured information from unauthorized access is known as confidentiality. The users will always fear about confidentiality aspect while their information is transferring to the cloud. In cloud confidentiality is connected with the areas such as intellectual property rights, covert channels, traffic flow analysis over the network, encryption techniques used to store the information and inference mechanisms.\\

\subsection\*{Integrity} Preserving the consistency and the correctness of the data is known as integrity. The cloud provider should ensure that unauthorized modifications are not made on the stored data.\\

\subsection\*{Availability} It ensures that the systems are functioning properly when needed. The users can able to use the cloud resources and systems when needed is termed as availability. DDoS attack is an example of a threat against availability in which they target the availability of networks, services and applications.\\

\subsection\*{Privacy issues} Since all the data from cloud users are stored in cloud data centers some issues may arise in the regard of privacy. Some privacy issues are loss of control, invalid storage, access control and data boundary.\\

To overcome the cloud security issues efficient security algorithms should be used by the cloud. Research should be carried out to make the cloud more secure. The relationship between data security concerns and the causes of data breach is shown in figure1.\\

\begin{figure}[htp]

\centering

\includegraphics[width=8cm]{1.png}

\caption{Primary Causes of Data Breach}

\label{fig:1}

\end{figure}

\subsection\*{ Security threats and challenges}

Cloud computing is having advantages such as easy implementation, accessibility, scalability, reliability, fault tolerance, shared resources, increased storage capacity and cost saving technology. Although Cloud computing has many advantages it comes up with lots of security issues and breaches faced by both cloud service providers and users. According to the Cloud Security Alliance paper, “data breaches, information misfortune, record or administration activity commandeering, shaky interfaces and Application Programming Interfaces (APIs), DoS attacks, malignant insiders, mishandle of cloud administrations, inadequate due tirelessness, lastly shared innovation vulnerabilities”, are identified as nine top most threats to cloud computing.\\

\subsection\*{Data Breach} A data breach is an activity which involves the unauthorized viewing, access or retrieval of data by an individual, application or service. It is a type of security breach designed to steal and/or publish sensitive data to an unsecured or illegal location. A data breach is also known as a data spill or data leak. Data leakage has become one of the greatest organizational risks from security standpoint. The reasons, including: Data corruption, Data being purposely or accidentally deleted or modified by a user or an attacker, Data stolen over the network by network penetration or any network intrusion attack, Data storage device physically damaged or stolen, Virus infection deleting one or more files.

\subsection\*{Account or Service Traffic Hijacking} Cloud account hacking is a procedure in which an individual or association's cloud record is stolen or captured by an assailant. Assault strategies, for example, phishing, extortion, and abuse of programming vulnerabilities are utilized by the aggressor to seize a record. By cloud account hijacking the attacker uses the stolen account information for unauthorized access to the user account. An attacker uses a compromised email account or other credentials to impersonate the account owner. \\

\subsection\*{Insecure Interfaces and Application Programming Interfaces (APIs)} Service provider demonstrates all the APIs that are utilized by the customer to connect with the cloud. Information course of action, personality administration, service checking, all happen on the cloud. Validation and get to control is inspected by these interfaces.\\

\subsection\*{Denial of Service (DOS)} In DOS attack, an attacker accomplishes spoofing and sends extensive number of solicitations to the server. So the server gets occupied and not ready to offer service to the valid user requests.\\

\subsection\*{Malicious Insiders} The employees who are working inside the company will do some malicious functions such as misuse the user or client information. This occurs inside of an enterprise and clients are uninformed of it.\\

\subsection\*{Abuse of Cloud Services} This threat arises due to relatively weak registration systems existing in the cloud computing environment. In cloud computing enrollment process, anybody having a legitimate charge card can enlist and utilize the services. This encourages obscurity, because of which spammer, vindictive code creators and culprits can assault the framework. Deficient Due Diligence An absence of due ingenuity is one of the top progressing dangers to cloud computing. While organizations may have a readiness of the general way of cloud innovation and related security threats, numerous organizations attempt minimal due perseverance about their cloud specialist organizations (CSPs). Indeed, even essential due steadiness, for example, assessing the money related soundness of the CSP or deciding the timeframe the CSP has been doing business, are frequently not cons diligence about their cloud service providers (CSPs). Even basic due diligence, such as evaluating the financial health of the CSP or determining the length of time the CSP has been in business, are often not considered. Ingredients of working underneath the cloud which make condition for registering does not bolster solid partition for multi execution mode. Among these threats, data breach is the most significant threat in the cloud computing technology. Data breaches to cloud services are increasing every year due to hackers who are trying to abuse the security vulnerabilities of the cloud. A data breach occurs when an unauthorized hacker or attacker accesses a secure database or repository of the user in the cloud. This security destruction may cause serious damage to the users’ data stored on the cloud. Data breaches can be occurred on logical or digital data over the internet or a network connection. A data breach may result in data loss, including the sensitive information stored on the cloud. A hacker may use the stolen data to imitate himself as the original user to gain access to a more secure location. For example, a hacker's data breach of login credentials of a net banking user can result in access of his entire account information.

\section\*{Security Approaches}

In this section, we examine some novel security approaches which are used in cloud computing organizations against data breaches.The primary issue is that with the presentation of the cloud; the cloud supplier has certain control over the cloud clients' information.

\begin{itemize}

\item \relax Information-centric security: For the ventures to oversee data in the cloud, it might be valuable to adopt a strategy of shielding information from within. This approach is called data driven security. This self-insurance procedure involves knowledge to be placed in the information itself. Data needs to act naturally portraying and ensuring, by the by of its environment. When got to, information checks its arrangement and tries to recreate a protected situation that is confirmed as dependable utilizing the structure of Trusted Computing (TC).

\item \relax High-assurance remote server attestation: At present, absence of transparency is keeping organizations from moving their information to the cloud. Information proprietors wish to look at how their information is being controlled at the cloud, and to affirm that their information is not being abused or spilled, or possibly have an unalterable review trail when it does happen. Currently, cloud suppliers are utilizing manual evaluating methods like SAS-70 to fulfill their customers. A way to deal with address this issue depends on trusted computing. In a put stock in processing condition, a trusted screen is introduced at the cloud server to screen the activities of the cloud server. The trusted screen gives a proof of consistence to the proprietor of the information, ensuring that specific get to approaches have not been violated. To guarantee honesty of the screen, secure bootstrapping of this screen keep running next to the working framework and applications.

\item \relax Privacy-enhanced business intelligence: A different approach to control data requires the encryption of all cloud data. The problem with this approach is that encryption restricts data use. Cryptographers have designed adaptable encryption proposals that take into account operations on the encrypted text. The cryptographic primitives, for example, homomorphic encryption (Gentry, 2009) and private data recovery (PIR) (Chor et al., 1998) perform calculations on cipher text without decrypting it. At the point when these cryptographic methods develop, they may open up new conceivable outcomes and directions for research for the development of cloud security algorithms.

\item \relax Privacy and data protection: Privacy is a main issue in cloud computing environment. It includes the need to protect identity information, policy components and transaction histories. By migrating workloads to a cloud infrastructure, sensitive information of the customer faces the risk of unauthorized access and exposure. All cloud security solutions must be embedded with privacy-protection mechanisms.

\item \relax Homomorphic encryption: This encryption scheme provides a mechanism to perform some specific type of computation on cipher-text which is not possible with any other encryption schemes. With this technique, data can be stored in the cloud as cipher-text format by the user cite{4}. They can perform any necessary computation without the need to decrypt the ciphertext.

\item \relax Searchable/ structured encryption: encryption is the base for this technique. It assures that the cloud does not know about the data and the computation which is performed on the data.

\item \relax Proofs of storage: It is a service level agreement between theCSPs and its clients. It ensures the data stored in the CSP’s servers would never be used by the CSP without the client’s permission.

\item \relax Server aided secure computation: This security mechanism offers a server and users to perform computation on the ciphertext without revealing the contents of the original data.

\item \relax Tools: Tools encompass data loss prevention systems, unusual behavior pattern detection tools, format preserving and encryption tools, user behavior profiling, decoy technology, and authentication and authorization technologies. These tools provide functions such as real-time detection on checking traffic, audit trails recording for future forensics, and trapping malicious activity into decoy documents to reduce the data breach issues.

\end{itemize}

\begin{figure}[htp]

\centering

\includegraphics[width=8cm]{2.png}

\caption{Relationship between Security threats,violation and data breach}

\label{fig:2}

\end{figure}

\section\*{Conclusion}

The security issue has turned into an obstacle limiting the applications of cloud computing in various fields. This paper concentrates on the significance of data breach issues in cloud computing. The research advance of issues of encryption, access control, and authentication et cetera as for data breach in cloud computing information security has been contemplated. Based on the study, we figure out the key technologies and key challenges the cloud computing data breach issues should be concerned about. Moreover, the research of cloud computing data breach problem is at the early stage of research. In terms of data breach problems in cloud computing data security, there are still a large number of key issues to be studied in depth which has been pointed out in this paper.

\\

\\

\\

\bibliographystyle{vancouver}

\bibliography{\jobname}

\begin{thebibliography}{9}

\bibitem{1}

Jitender Grover, Shikha, Mohit Sharma

\textit{Cloud Computing and Its Security Issues – A Review}.

2014,IEEE 5th ICCCNT

\bibitem{2}

D.Chandramohan,T.Vengattaraman,D.Rajaguru,R.Baskaran, and P.Dhavachelvan

\\\texttt{A Privacy Breach

Preventing and Mitigation Methodology For Cloud Service Data Storage}2013 3rd IEEE International Advance Computing Conference (IACC)

\bibitem{3}

Justin LeJeune, Cara Tunstall, Kuo-pao Yang, IhssanAlkadi, 2016 IEEE

\textit{An Algorithmic Approach

to Improving Cloud Security: The MIST and Malachi Algorithms}2016.

\bibitem{4}

MounaJouini, Latifa Ben ArfaRabai

\textit{Surveying and Analyzing Security Problems in Cloud Computing Environments”,2014.}2014,IEEE 10th International Conference on Computational

Intelligence and Security.

\end{thebibliography}

\bibliographystyle{vancouver}

\bibliography{\jobname}

\end{document}