A Novel Model to Secure ERP in a Cloud Computing Environment

[1]Naveen Chandra, [2]Dr. Manoj Kapil
[1]Research Scholar, [2]Principal,
Subharti Institute of Technology & Engineering
Swami Vivekanand Subharti University, Meerut, UP, India

Abstract: Information is the goal of the ERP implementation, and both strategy and capable resources are required to achieve this goal. For any enterprise application there can be internal users and external users. External users are consumers from which any system gains profit where as there are Internal Users and applications used within the organization. The internal applications are very much weak because when employees perform the task there is a mutual understanding regarding the tasks and co-workers share among themselves. Hence an approach is needed to perform the audits of various actions and then identify suspicious actions and events.

Index Terms **- ERP, KPIs, LCS, OTP, TF-IDF, Cloud, Security.**

I. INTRODUCTION

Structures, for example, solicitations, request affirmations, buy orders, receivables explanations, payables checks, and so on. Overseen reports delivered on a reoccurring premise Specially appointed reports that are typically one-time, "I need this data presently" reports Systematic reports that show information and help investigate what's going on Official dashboards that give a depiction of business execution against the organization's key execution pointers (KPIs).These things should be considered in building up a verified cloud ERP. The various security feature in existing ERP systems has been studied and based on that the system is dev loped to provide an enhanced secured cloud ERP based system. The security aspects of the system with the main focus on providing intrusion detection facility towards internal abrupt usage has been the key research aspect of this research work. The security features thus incorporated and algorithm has been explained in the below sections.

II. SECURITY FEATURES

Secure from update and deletion of data

If any unauthorized user want to delete or update data system send a OTP(one time pass word) to authorized mail id when user enter that OTP then he/she will be able to access account.

Secure Login

If authorized user logout from the device(secure user login from their system) by this featured on login a log file will be generated which will store all related information in that file like as System IP,HD no (which is one user registered),and cookies (like web browser details)

Authority and Key Distributions

The admin module is responsible for defining the users especially responsible for internal testing of the application and the short description of the tasks which users have to perform.

Monitoring and Filtering Algorithm

The event logs and sequence logs are considered and then the algorithm computes the following for each sequence of events per user independently by using a scheduler. The algorithm computes the following per user text frequency, inverse document frequency and TF-IDF.

Computation of Weights

The Text Frequency is represented using the following equation

$$TF = \frac{n_i}{\sum_{i=1}^{N_j} n_j}$$

where,

$n = number\ of\ times\ a\ command / action\ is\ repeated$

The Inverse Document Frequency is computed using the following equation

$$IDFT = \log(\frac{D}{n})$$

Where,

$D = Number\ of\ sessions\ in\ which\ the\ action\ is\ present$

$n = count\ of\ word\ in\ a\ session$

The TF-IDF is computed using the following equation

$$TF - IDF = TF_i * IDFT_i$$

User Habit File

1) Set of Log Sessions
2) Find the Maximum Session Length
3) Compute LCS from Maximum Session Length to every other string sequence
4) Like this we get LCS patterns for User
5) Once we get the LCS pattern which is matching then compute the frequency
6) Otherwise for unique LCS pattern assign the value as 1

Note here the a given Session is divided into 10 sub sections

Secure Data

If any want to enter into account a mail will be send to authorized user with system ip,HD Number, time ,and location like as a record .

III. Detection of Internal Attacker

The internal attacker identification is performed by using the following algorithm

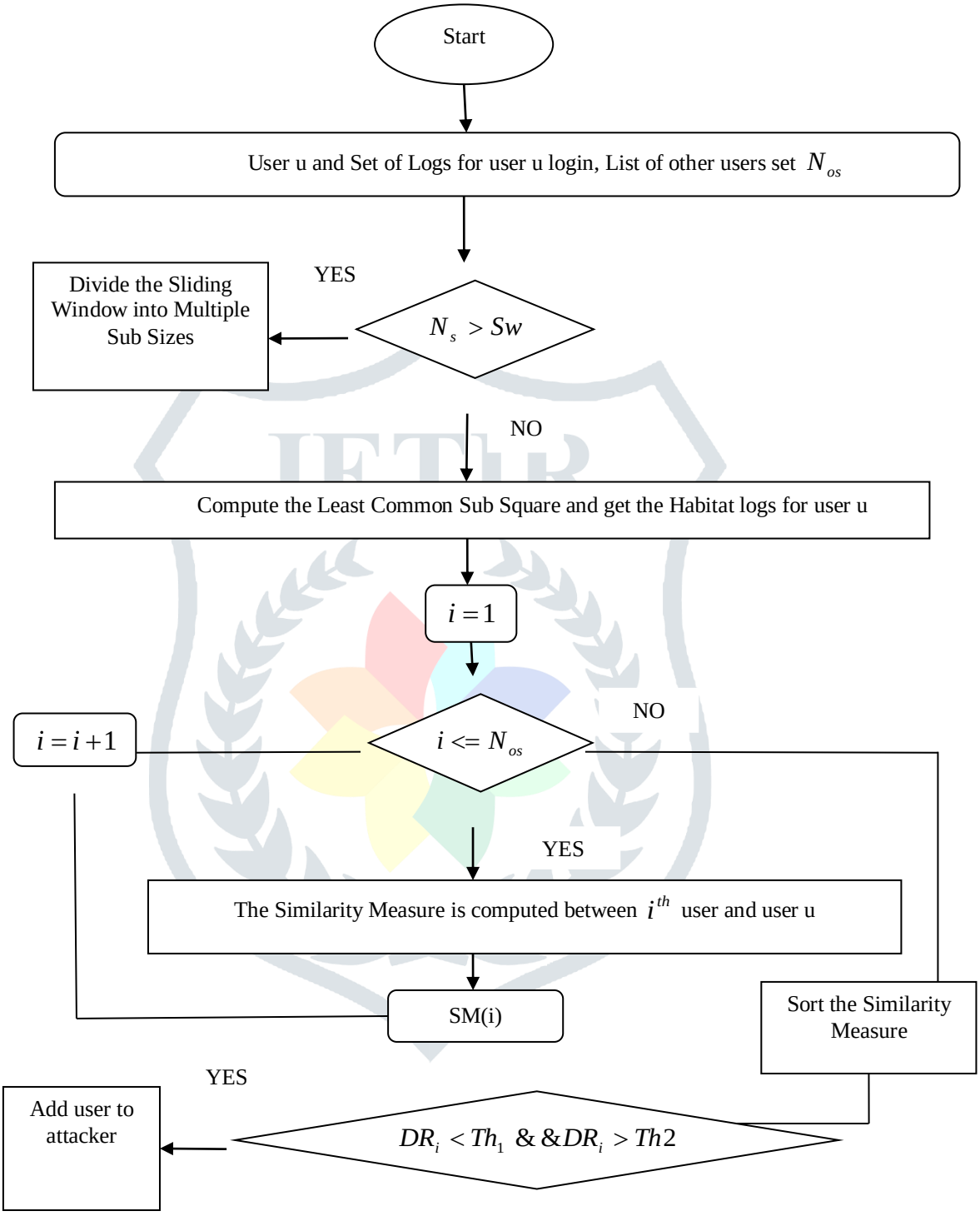


Figure 1: Internal attacker identification algorithm

The threshold and similarity measure is described is as below:

$$sim(u,i) = \sum_{i=1}^{p} F_{iu} W_{ij}$$

$$Where,$$
$$p = Number\ of\ \ patterns$$
$$F = apperance\, count\ of\ \ pattern$$
$$W = weight\ \ pattern$$

The weight computation is given by

$$W_{ij} = \frac{f_{ij}}{f_{ij} + 0.5 + \frac{1.5 ns_j}{ns_{avg}}} \quad \frac{\log(\frac{N+0.5}{M_i})}{\log(N+1)}$$

$$i = 1,2,3,4,.....k$$
$$j = 1,2,3,4,.....N$$

Where,

$$f_{ij} = frequency\ of\ \ apperance\ of\ \ Command / Action$$
$$ns_j = total\ number\ of\ \ patterns\ of\ \ user$$
$$ns_{avg} = average\ number\ of\ \ patterns\ across\ users$$
$$M_i = Number\ of\ \ user\ patterns$$

$$threshold1 = predefined\ threshold\ \ for\ the\ Least\ Common\ Subsquare\ for\ user\ u$$
$$threshold2 = predefined\ threshold\ \ for\ the\ Least\ Common\ Subsquare\ to\ belong\ to\ \ attac\text{ker}$$

IV. LEAST COMMON SUB SQUARE ALGORITHM

1) Consider the sequences namely $S1\ and\ S2$
2) The length of S1 and length of S2 is computed
3) Find the maximum length of S1 and S2
4) Construct a matrix initial with zeros one 1st row and 1st column
5) If the value of the sequence alphabet is not there then maximum on top and left is taken
6) If the value matches then diagonal value is increment by a value of 1

The best way to dodge such assaults is to rehearse great programming systems. Framework level security can be given utilizing better firewalls. Utilizing interruption identification and avoidance can likewise help in preventing assailants from simple access to the framework. For this purpose we used some special technique to avoid hacking of system and moderate the whole system in featured way. Some basic concepts used in this research project are as below:

i) Login time security
ii) Updating time security
iii) Deleting time security

Login time security:

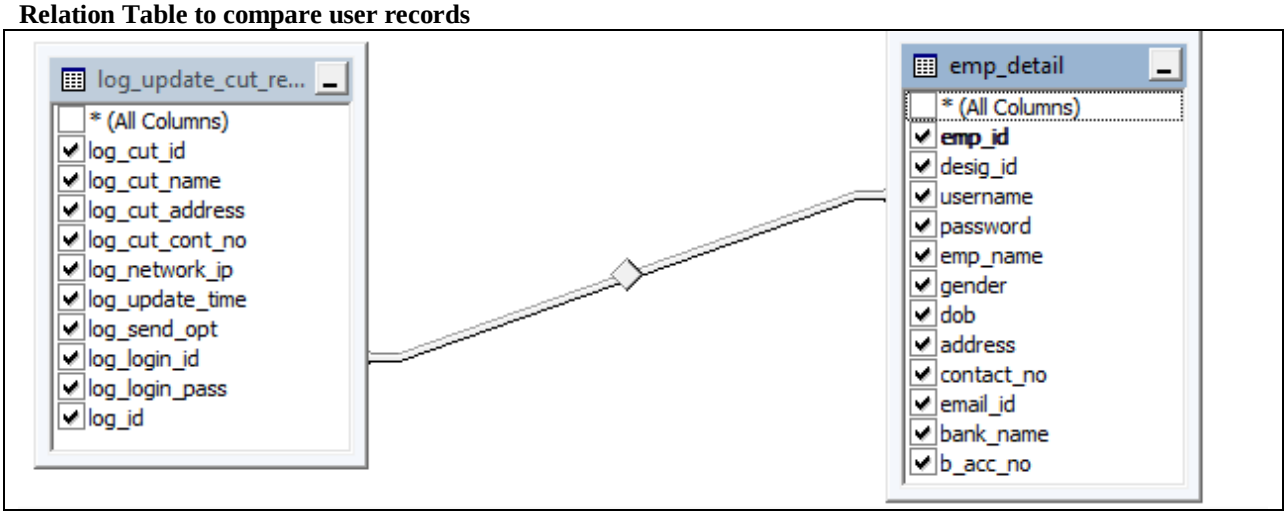
This is two way process in case if unauthorized user want to access any one account using authority database (like User Id , User password) this process send an information just like System Name and System IP to registered user's email. System will automatic detect a user is authorized or not by using pattern log file.

Pattern Log File:

Pattern log file store all the information about system and user information on the time of login and logout. A regular user will start working on a account at a particular time and from particular system but in case some other want to access then the system send all the related information to registered user email id.

Column Name	Data Type	Allow Nulls
loginid	int	☐
login_time	nvarchar(MAX)	☑
logout_time	nvarchar(MAX)	☑
system_name	nvarchar(MAX)	☑
login_userid	nvarchar(MAX)	☑
login_userpass	nvarchar(MAX)	☑
		☐

Relation Table to compare user records



Column	Alias	Table	Output	Sort Type	Sort Order	Filter	Or...	Or...	Or...
emp_id		emp_detail	☑						
desig_id		emp_detail	☑						
username		emp_detail	☑						
password		emp_detail	☑						
emp_name		emp_detail	☑						
gender		emp_detail	☑						
dob		emp_detail	☑						
address		emp_detail	☑						
contact_no		emp_detail	☑						
email_id		emp_detail	☑						
bank_name		emp_detail	☑						
b_acc_no		emp_detail	☑						
log_cut_id		log_updat...	☑						
log_cut_name		log_updat...	☑						
log_cut_address		log_updat...	☑						
log_cut_cont_no		log_updat...	☑						
log_network_ip		log_updat...	☑						
log_update_time		log_updat...	☑						
log_send_opt		log_updat...	☑						
log_login_id		log_updat...	☑						
log_login_pass		log_updat...	☑						
log_id		log_updat...	☑						
username	Expr1	emp_detail	☑						

Updating time security

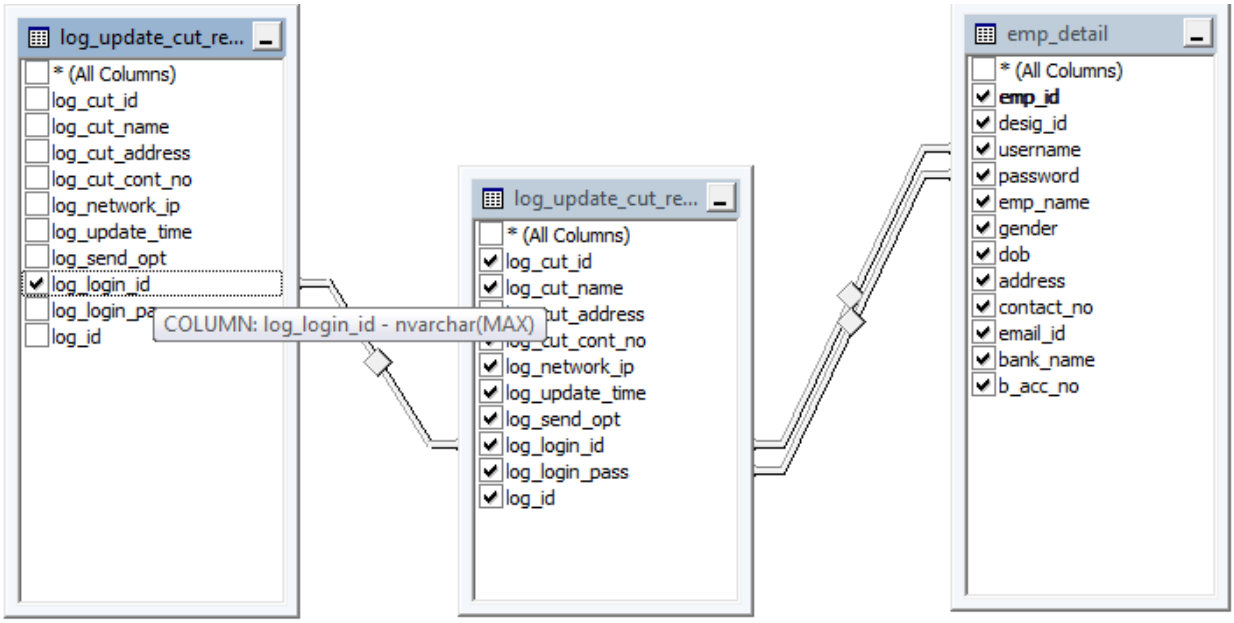
It's a second level security if any user authorized user enter by any mean and want to update a record but he was unable to update data because webpage send a OTP* to registered user on email .the updating process will not be complete until valid OTP is not entered but if user is hacker and hacked whole website then he can change the email so we create a log file to protect data in LOG file .If authorized find some bugs he can restore data from log file hence it's a more secure process to all.

Deleting time security

A one-time password (OTP) isa naturally created numeric or alphanumeric series of characters that validates the client for a solitary exchange or session. An OTP is more secure than a static secret key, particularly a client made secret key, which is commonly powerless. OTPs may supplant validation login data or might be utilized notwithstanding it, to include another layer of security.

OTP tokens are normally stash measure coxcombs with a little screen that shows a number. The number changes each 30 or 60 seconds, contingent upon how the token is designed. For two-factor authentication, the user enters his user ID, PIN and the OTP to access the system.

Comparison table after Deleting and updating record:



In the complete process a log file stores the updated data in log file and user record by the above query we will fetch all the data information like the which table is updated and which user update the record here its become more secure than from unauthorized user.

log_update_cut_record

Column Name	Condensed Type	Nullable	Length	Precision
log_cut_id	nvarchar(MAX)	No	-1	0
log_cut_name	nvarchar(MAX)	No	-1	0
log_cut_ad...	nvarchar(MAX)	No	-1	0
log_cut_co...	nvarchar(MAX)	No	-1	0
log_networ...	nvarchar(MAX)	No	-1	0
log_update...	nvarchar(MAX)	No	-1	0
log_send_opt	nvarchar(MAX)	No	-1	0
log_login_id	nvarchar(MAX)	No	-1	0
log_login_p...	nvarchar(MAX)	No	-1	0
log_id	int	No	4	10

emp_detail

Column Name	Condensed Type	Nullable	Length	Precision
emp_id	int	No	emp_detail	10
desig_id	int	No	4	10
username	varchar(30)	No	30	0
password	varchar(30)	No	30	0
emp_name	varchar(50)	No	50	0
gender	char(1)	No	1	0
dob	datetime	No	8	23
address	varchar(50)	No	50	0
contact_no	varchar(30)	No	30	0
email_id	varchar(50)	No	50	0
bank_name	varchar(50)	No	50	0
b_acc_no	bigint	No	8	19

V. COMPARISION GRAPH

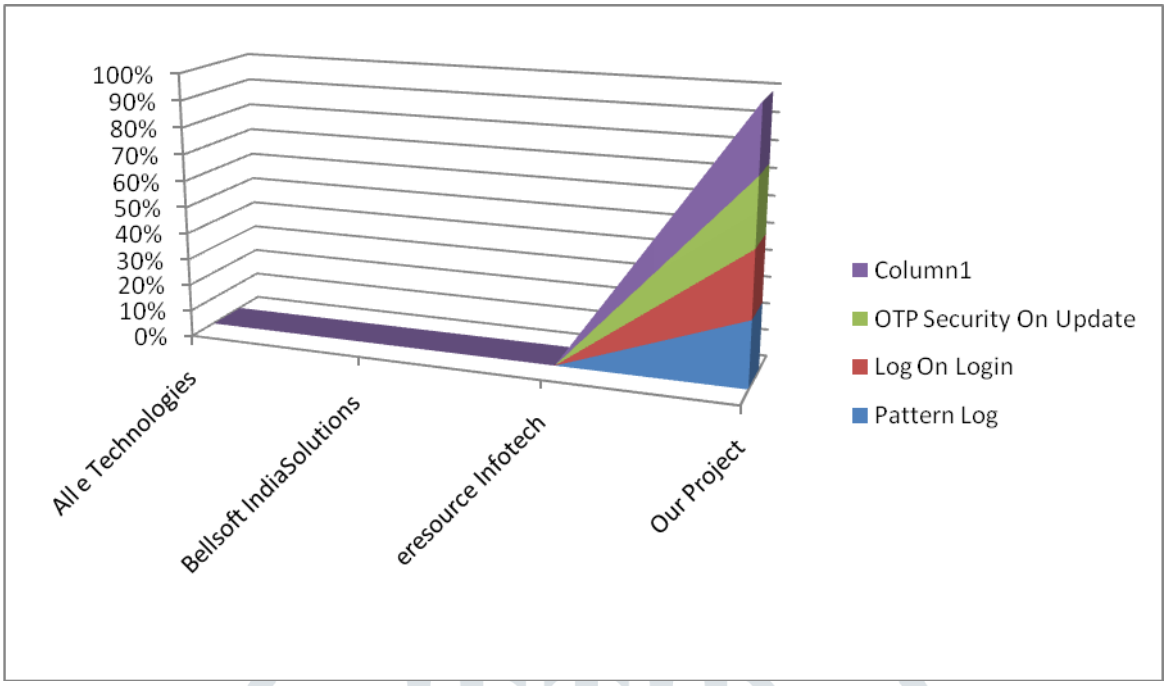


Figure 2: Comparison graph-A

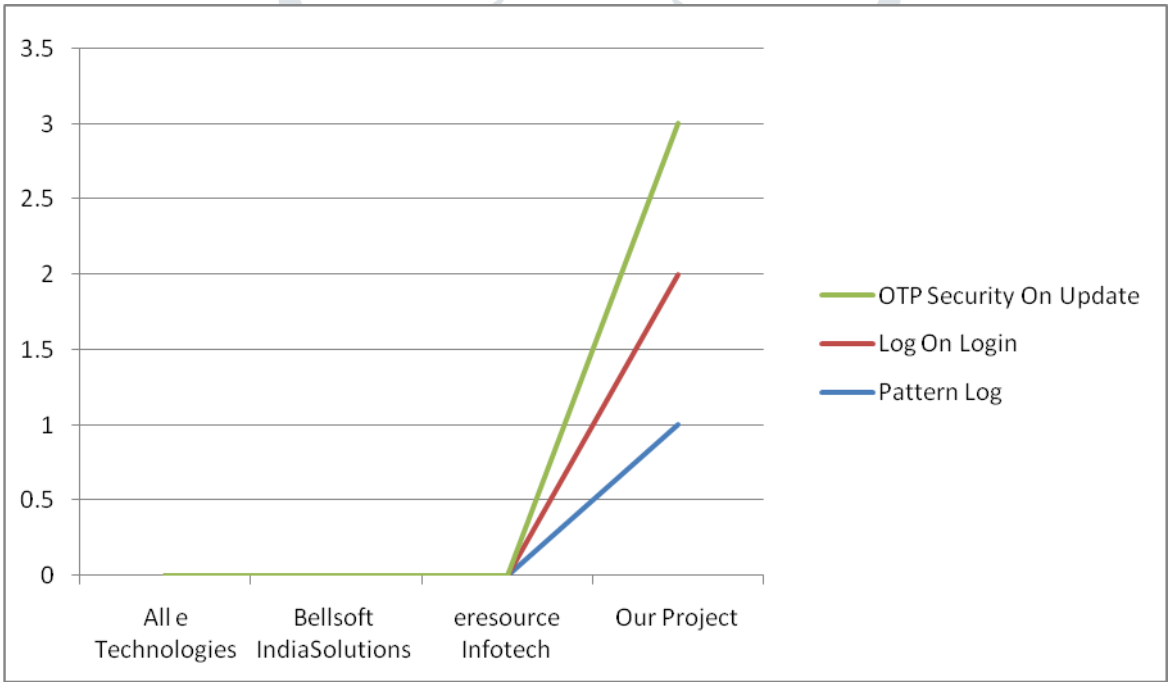


Figure 3: Comparison graph-B

VI. CONCLUSION

In this thesis we have tried to compare the performance of Cloud Based ERP with Traditional ERP system. The principle distinguished advantages of cloud-based ERP in examination with customary ERP are lower forthright costs, lower working expenses and more internal secure environment. Naveen Chandra, quick usage, and versatility, center around center capabilities, fast updates and overhauls, improved availability, portability, and ease of use, simpler mix with cloud benefits, and improved catastrophe recuperation. Here we have explained the flexibility offered by cloud ERP systems. All the data stored at different locations can be easily grouped together and more secure from internal threats. Reports can be generated and analyzed efficiently. All the applications can be integrated and maintenance becomes simple.

Before moving to the cloud ERP system, the cloud ERP clients should balance between benefits and challenges. One benefit could lead to numerous difficulties and on another side, a few difficulties cloud be settled by certain advantages. The high appraised difficulties speak to investigate focuses, which ought to be considered to improve the usage and activity of cloud ERP frameworks.

VII. FUTURE SCOPE

Cloud ERP profoundly affects the whole IT industry as another plan of action. Incorporated into all areas of business applications, Cloud ERP will mirror the incentive in a more profound dimension. With the fast improvement of Cloud ERP, it can help undertakings to get to superior IT administrations with lower cost, and furthermore helpful for little and medium-sized ventures to get to elite IT administrations like expansive endeavors. In the meantime, its decrease weight can help endeavors to focus on its center business.

The procedure advancement which dependent on Cloud ERP can accomplish all through an extensive scale recreation of the business, and improve the general IT norms and aggressiveness. Here are some different reasons why each venture may require Cloud ERP for their business: Cost reserve funds - Cloud processing evacuates the necessity of an organization to put resources into capacity equipment and servers. Focusing on the business - Since all of the organizations will execute over the web, an association does not have to make a big deal about specialized issues and different issues related with physical capacity and reinforcement. An organization would thus be able to concentrate more on their center business. We focused more on internal security threats in this research work, more emphasis is required on external security threats in future. Execution - It conveys dependable execution regardless to the topographical area of the client. Another key element could be the programmed refreshing of administrations and applications. Security - Cloud Computing offers perfect security which guarantees you against any unapproved access, modification and loss of data. Adaptability - Even if part of the cloud condition falls flat or quits working, different assets keep on working until the issue is fixed.

REFERENCES

[1]. Zhao G, Liu J, Tang Y, Sun W, Zhang F, Ye X, Tang N (2009) Cloud Computing: A Statistics Aspect of Users. First International Conference on Cloud Computing (CloudCom), Beijing, China. Springer Berlin, Heidelberg, pp. 347-358.

[2]. Zhang S, Zhang S, Chen X, Huo X(2010) Cloud Computing Research and Development Trend in Second International Conference on Future Networks, Sanya, Henan, China, IEEE Computer Society, Washington, DC, USA, pp. 93-97

[3]. B R. Kandukuri, R. Paturi V.and A. Rakshit, "Cloud Security Issues," 2009 IEEE International Conference on Services Computing, Sep 21-25,2009, Bangalore, India, pp. 517-520.

[4]. E. H. Spafford and D. Zamboni, "Intrusion Detection Using Autonomous Agent," Computer Networks, Vol. 34, Issue 4, 2000, pp. 547-570.

[5]. Ms. Parag K. Shelke, Ms. Sneha Sontakke, Dr. A. D. Gawande,"Intrusion Detection System for Cloud Computing", International Journal of Scientific & Technology Research, Vol. 1, Issue 4,May 2012, pp. 67-71.

[6]. Chi-Chun Lo, Chun-Chieh Huang, Joy Ku, "A Cooperative Intrusion Detection System Framework for Clouding Computing Networks," 2010, 39th International Conference on Parallel Processing Workshops, pp. 280-284.

[7]. Anna Lenart, "ERP in the Cloud- Benefits and Challenges,"Springer Verlag Berlin Heidelberg, 2011, pp. 39-50.

[8]. C. Modi, D. Patel, B. Borisaniya, H. Patel, M. Rajarajan, "A Survey".

[9]. Gartner Inc. Gartner identifies the Top 10 strategic technologies for 2011. Online. Available: ttp://www.gartner.com/it/page.jsp?id=1454221. Accessed:15-Jul-2011

[10]. Cloud Security Alliance (2011) Security guidance for critical areas of focus in Cloud Computing V3.0.. Available: https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

[11]. Subashini S, Kavitha V (2011) A survey on Security issues in service delivery models of Cloud Computing. J Netw Comput Appl 34(1):1–11

[12]. Mell P, Grance T (2011) The NIST definition of Cloud Computing. NIST, Special Publication 800–145, Gaithersburg, MD

[13]. Zhang Q, Cheng L, Boutaba R (2010) Cloud Computing: state-of-the-art and research challenges. Journal of Internet Services Applications 1(1):7–18

[14]. National Institute of Standards and Technology (NIST) Definition of Cloud Computing. (n.d.). Retrieved from http://csrc.nist.gov/groups/SNS/cloudcomputing/

[15]. KeJing Zhang, PingJun Dong, Biao Ma, BingYong Tang, Hong Cai, ―Innovation of IT Service in Textile Industrial Clusters from the Service System Perspective‖, 2010 IEEE, p 1819-1822.