encrypted format. "The security lapse occurred on two levels: both the data itself (being unencrypted) and the physical location (stored in an unsecure location)[7].

5) Tricare and SAIC

In September, backup tapes containing SAIC (Science Applications International Corporation) data were stolen from the car of a Tricare employee. The breach led to a $4.9 billion lawsuit being filed, which aims to award $1,000 to each of the 5.1 million people affected by the breach. "The Tricare/SAIC breach is significant because not only are the victims at risk of medical identity theft, but financial identity theft as well.

4.3 Year 2012

1) University Of North Carlolina

The data benchers stole bank accounts and social security numbers for roughly 350,000 students, staff and faculty members. This is occurred, due to misconfigured security settings.

2) LinkedIn

Social networking powerhouse, LinkedIn, was tapped for approximately 6.5 million unsalted SHA-1 hashed passwords posted to the Internet. Even also the hackers published them publicly in order to use the buddy system.

3) Yahoo

More than 400,000 plaintext passwords were lifted from Yahoo and subsequently posted on the Internet. Whi most of the passwords seem to have been taken from t Yahoo voice services.

4) Global Payments: $84.4 million data breached

Credit card processor Global Payments at the end of March disclosed a breach that exposed 1.5 million consumers to fraud. The breach, which was under scrutiny by federal investigators, exposed credit card numbers, user PINs and other data but not credit card holders' names, addresses or social security numbers.

4.4 Year 2013

1) Zendesk Breach

Zendesk, which provides customer support messages to users of Twitter, Tumblr and Pinterest, announced a data breach in February that impacted its clients. The breach exposed thousands of email addresses and support messages from users of the services.

2) Twitter Breach

Twitter recently rolled out support for two-factor authentication to bolster the security of its user base [11]. Attacker exposed the usernames, email addresses and encrypted passwords of 250,000 users.

3) Vendini ticketing

Hackers focused last spring on breaking into the Vendini ticketing system in use by various organizations in order to steal customer financial data.

4) Piedmont HealthCare

Social Security numbers, on 10,000 job applicants was stolen due to a hacker and at the same time, Presbyterian Anesthesia Associates there disclosed a hacker apparently exploited a vulnerability flaw in its website to gain access to a database of information on about 10,000 patients who had their credit-card information stolen.

4.5 Year 2014

1) Social media giants Facebook, LinkedIn, among others, get hacked…repeatedly.

Twitter, Pinterest and Tumblr inadvertently suffered a breach after their customer service provider, Zendesk, got hacked [10]. No passwords were compromised but thousands of user emails were obtained and likely would have been used in email phishing scams to get more personal information.

Hackers stole usernames and passwords for nearly 2 million accounts at Facebook, Google, Yahoo, LinkedIn, Twitter and 93,000 other websites. That breach was a result of malware installed on user computers that swiped log-in credentials for thousands of sites for over a month. Facebook accounts were compromised the most, followed by Google, including Gmail and YouTube.

arly 40 million Target customers' credit and debit card numbers were stolen in midst of holiday shopping rush.

Cyber-thieves stole Target store shoppers' credit card numbers and debit card PINs—the four-digit number used to access bank accounts[9].

3) Adobe breach snowballs into multi-network security risk.

Adobe reported that 3 million customers' credit card information was stolen. A source code leak also exposed almost 40 million user emails and passwords [8]. But the breach's affect spanned beyond Adobe's Photoshop users.

4) System bug exposes 6 million Facebook users' personal data in yearlong breach.

Facebook said the leaks, which began in 2012, were the result of a technical glitch that was corrected in June.

4.6 Year 2015

1) Anthem Inc

The nation's second largest health insurer disclosed that hackers had broken into its servers and stolen Social

Security numbers and other personal data from all of its business lines. Given the company's size, this breach could end up impacting tens of millions of Americans.

2. Conclusion

With the immense growth in the popularity of cloud computing security have become important concerns. The objective of this paper is to understand how and what type of data breaches occurs in cloud. In this paper we also discuss how the organization affects from these data breaches. Future work will include the prevention against these data breaches.

References

[1] Definition - What does Data Breach mean
[2] http://www.oriontech.com/wp-content/uploads/2015/02/Orion_LogoMark-Favicon.png
[3] Most Common Causes of Data Breaches - Orion Blog.htm
[4] Data Breach - Definition - Trend Micro USA.htm
[5] Anatomy of a Data Breach - Threat Encyclopedia - Trend Micro USA.htm
[6] http://www.informationweek.com/news/security/client/230500044
[7] http://www.informationweek.com/news/security/attacks/229301337
[8] http://www.informationweek.com/news/security/government/229700300
[9] http://bits.blogs.nytimes.com/2013/11/12/adobe-breach-inadvertently-tied-to-other-accounts/
[10] http://thinkprogress.org/economy/2013/12/23/3101291/target-breach-highlights-lack-uniform-consumer-protections/
[11] http://newsfeed.time.com/2013/12/13/youve-made-it-your-leaked-linkedin-password-is-now-hanging-in-n-art-gallery/
[12] https://blog.twitter.com/2013/keeping-our-users-secure
[13] Worst Data Breaches - The Court Ventures hack of 2012 appears to be the biggest hack in history, in terms of number of records stolen."
[14] http://en.wikipedia.org/wiki/Cloud_computing