International Journal of Pure and Applied Mathematics
Volume 119 No. 14 2018, 19-28
ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

DATA BREACHES AS TOP SECURITY CONCERN IN CLOUD COMPUTING

Govind Rao Mettu[1] Dr Anitha Patil[2]

Computer Engineering,Pillai HOC College of Engineering and Technology,Rsayani, Inida
Computer Engineering,Pillai HOC College of Engineering and Technology,Rsayani, Inida

Abstract

Data breach is an incident that has potential to disclose sensitive information to an unauthorized party. Data breaches may be caused by a variety of reasons such as theft. In the era of cloud computing, data breaches is one of the major security concerns found in the literature. There were plenty of incidents of this kind in the history of computing and of late the cloud computing. Since cloud computing is the technology that delivers on-demand services pertaining to infrastructure, software and platforms, it is vulnerable various kinds of data breaches. Unless there is assurance to have security mechanisms in place, data owners express security concerns to outsource their data to public cloud. Though cloud service providers are striving to ensure protection of data of their customers, there were sufficient incidents related to data breaches that caused trouble to most reputed companies as well. Keeping the importance of this in mind, in this paper, we make a review of literature on the data breaches in cloud computing. Then we proposed a methodology for end to end secure communications through encryption. The proposed method does not allow an adversary to gain any meaning from stolen information as the content is encrypted and needs security credentials. The method is compared with other schemes found in the literature. The results revealed that the proposed method is better than other state-of-the-art schemes.

Index Terms – Cloud computing, security, data breaches, cryptography

1. INTRODUCTION

Data breach is an incident where confidential information is viewed or stolen by unauthorized people. There might be attacks that are launched with data breach as their primary objective. Data breaches may occur due to human error, poor security settings and vulnerabilities that exist in the applications being used. The information disclosed due to data breach may involve information that is not meant for public release. Such sensitive information may be personally identifiable information (PII), intellectual property, trade secrets, financial information, and personal health information and so on. Cloud based data of an organization may be required by many genuine parties for various reasons. Apart from this there might be an organized crime that needs personal, health and financial information with malicious intentions. Sometimes, foreign nationals and business competitors might need confidential information of other organizations to know their trade secrets and gain benefit from such information. Even adversaries may want to expose sensitive information to cause embarrassment and damage to organizations. Interestingly it is possible that unauthorized insiders may steal organization's sensitive data which is actually major concern among different countries. This paper is talking about data breaches in cloud computing. However, such risk is not limited to cloud computing. But consistently cloud customers are victims of data breaches. The rationale behind this is that cloud is in distributed environment where threats come from traditional sources and also shared resource besides personnel of cloud service provider. As the cloud service provider is associated with different parties for services, it may because issues related to data breaches. Moreover, cloud provides vast amount of resources that are highly accessible and they are attractive targets to attacks. Every data breach has associated problem. However, the degree of problem is determined by the level of sensitivity of the data subjected to data breach. There are laws enforced in different countries causing companies to follow certain security standards to protect sensitive information. These laws cause large fines and civil and criminal cases when data breach cases arise in organizations. When data breach occurs, the company also need to pay for the cost of data breach investigations and notify customers affected by the data breach. Some companies in the real world have professional consulting and services related to law to have better response when a breach occurs. The company which is subjected to data breach fraud can also take the services from credit monitoring when consumers lost their data and the data is misused by adversaries. There are certain indirect impacts of data breach. For instance, the brand image of the company may be deteriorated and continuing in the business may

become hard. Customers may leave the organization and acquiring new users may incur cost to the organization. It is known that cloud service providers are striving to provide good security to the data being outsourced to cloud. An effective security program may provide best protection against data breach. There are two important security measures to stay secure are encryption and multi-factor authentication. In this paper we proposed a security scheme based on cryptography. The scheme is proved to be efficient and can be used for mitigating data breaches in cloud computing. The remainder of the paper is structured as follows. Section 2 presents review of literature. Section provides examples of data breaches. Section 4 covers encryption to minimize data breach. Section 5 focuses on the data breaches in cloud based storage facilities. Section 6 covers the role of stolen passwords in data breaches reported so far. Section 7 describes the popular trends in data breaches. Section 8 describes different ways to avoid data breaches. Section 9 presents the proposed key management scheme for mitigating data breaches. Section 10 presents experimental results. Section 11 concludes the paper besides providing directions for future work.

2. REVIEW OF LITERATURE

This section makes a review of literature related to data breeches and security concerns. Cloud computing is a new mode of computing [25]. A survey on security issues and different solutions for cloud computing security is found in [1]. Various cloud security issues and case studies are reviewed in [2]. Similar kind of research carried out in [3], [6], [8], [9], [10], [14], [20], and [24]. Various security vulnerabilities and security threats are discussed in [4] related to cloud computing. It is found that there is risk associated with cloud computing. The risk perception and risk assessment in cloud computing was the study in [5].

Various counter measures for security threats identified in cloud computing are presented in [11] which critical infrastructure security issues are provided in [12]. Vulnerabilities related to hypervisors used in cloud computing are discussed in [13]. When cloud computing is used by small companies, there might be different security risks due to lack of security primitives in place. Such potential threats in cloud computing are discussed in [15]. Cloud computing with Internet of things, trust based security and security issues in the cloud are investigated in [16], [17] and [18] respectively. Quantitative measures of information security [19], security threats in cloud computing [21], distributing environment and security challenges [22], information privacy and its protection [23], taxonomy of security aspects in cloud computing [26], security threats mapping [27], privacy, security and integrity in cloud computing [28] are other important contributions in cloud computing security. Similar kind of work is found in [29] and [30]. In this paper we provide various data breach cases and provide a methodology for data breach prevention.

3. EXAMPLES OF DATA BREACHES

There are many good examples of data breaches. An antivirus firm known as BitDefender in the year 2015 had security vulnerability due to which its customers' credentials such as username and password were stolen. It happened in its public cloud application deployed on AWS. The hacker behind this data breach demanded the company $15,000 [34]. Another data breach known as Anthem breach surfaced in the same year. It caused the private information of more than 80 million customers to be breached. When the company is outsourcing the customer data to public cloud, in the transit, the data breach occurred [32]. TalkTalk is a British telecom provider who found many incidents of data breach in 2014 and 2015. It involved the theft of personal information of its four million customers. These data breaches are followed by scam calls in order to extract sensitive information related to banking from TalkTalk customers. TalkTalk was criticised for these attacks ass it failure to provide cryptographic security to its customers' data [35].

4. ENCRYPTION TO MINIMIZE DATA BREACH

Adobe in the year 2013 lost control of as many as 38 million records of its customers due to data breach. It was found very band for the company as the data breached contained credit and debit cards as well. Later on it was understood that the breach caused the disclosure of 150 million credentials. Some months later another data breach occurred which is bigger than that of Adobe's. It occurred and caused loss of credit and debit cards of more than 70 million customers including CVV codes. This data breach causes loss of around $148 million. Of late, JPMorgan, eBay and Home Depot are the companies that were the victims of data breaches. In all the data breaches, circumstances varied but there is one common thing that is when the data is encrypted, the stolen data is not useful to hackers [40]. Therefore it is important to have sensitive data to be encrypted. Especially it is essential to encrypt data such as card PINs as they are able to help adversaries to gain financial benefits. It can be avoided by encrypting PINs

when they are being exchanged electronically. It is also possible to hash credentials and protect them from thieves. The reason behind this is that hashed passwords have similar effect of encryption and such passwords cannot be reversible and do not help attackers. Data is like water which causes leakage. It tends to move places without constraints. Even it is true that when data is not used by intended parties, it is of no value. There should be balance between the data utility and security to prevent data breaches. Data needs to be used by authorized parties and at the same time prevent accessing by unauthorized people. With respect to cloud, it can be compared with a big lake in the middle of the world and people all over the world can access it in pay per use fashion. As cloud is given public access, there is more scope for data breaches. It needs to be prevented in such a way that only authorized people can access data. It is very challenging task to prevent data breaches. As mentioned above encryption is widely used security measure that can restrict access to data and make the data useless to hackers unless they have key to decrypt it. Cyber criminals are restricted from unauthorized access as the PINs are hashed or encrypted. At the same time, it is not feasible to encrypt everything. It is too hard is the expression posed by organizational historically with respect to encrypting everything. Though encryption solves the problem of protecting sensitive data, there is an issue with it. When keys are lost, everything is lost. The rationale behind this is that when a person controls keys can easily control data. Indirectly it says that when data is not encrypted, you do not have the chance of controlling keys and the data as well. When data is encrypted, it potential value is lost in its current form unless the key to decrypt is known. This is mitigating risk to a great extent. Though encryption has its own challenges and risks, it is essential to face then to protect data, organizations and careers at large. Well-known encryption technologies are to be used in order to protect data of cloud. Data breaches are not technical problems; they are the result of security lapses in organizations. Effective key management and encryption can mitigate data breaches as much as possible. Though encryption cannot address all issues related to data breaches, it is essentially a step forward in the correct direction.

5. DATA BREACHES IN CLOUD BASED STORAGE FACILITIES

Box and Dropbox are cloud based storage facilities that provide on-demand infrastructure services. In these online storage platforms, a major vulnerability has been identified that is related to file transfer links that are private in nature. It does mean that the private data is indexed by search engines and misused by third parties. The cloud based file locker known as Intralinks was victim of data breach with respect to Google AdWords campaign. The competitors such as Box and Dropbox were identified using such services advertised and the underlying keywords. Vulnerability was found when users used share links in order to share file and then the links were inserted into search box in browser. This has allowed Intralinks to obtain campaign management interface of AdWords. Similarly users of those storage facilities are vulnerable to slightly different attacks [31]. The security features of Box and Dropbox depend on the security knowledge of end users to protect sensitive data. When users do not have such knowledge, it results in data breaches. Moreover, business users of Dropbox do not find an option to restrict shared link access when users of Box do have some features related to restrictions and password protection. In 2014, Dropbox accounted the measures to protect users' shared links and avoid vulnerabilities. They helped users to generate links that are not susceptible.

Even browsers can play an important role in preventing data breaches. Towards this end popular browsers made design changes in the way people interact with browsers. For instance Google chrome did its research on the removal of length URLs and display only domain names. Theoretically, this kind of measure of the chrome could prevent phishing as people cannot understand the links easily and do not indulge in performing phishing attacks. In the same fashion, Mozilla Firefox has a feature to protect user when the URL appears to be malformed. It separates the search boxes and address otherwise it may cause vulnerability with cloud storage facilities such as Box and Dropbox.

6. ROLE OF STOLEN PASSWORDS IN ALL DATA BREACHES

There might be different reasons for each data breach. But the research found that stolen passwords have been causing significant number of breaches from time to time. According to Verizon Data Breach Investigations Report (DBIR) in 2014, every two breaches out of three were caused by stolen credentials. Adversaries try to get sensitive information such a user id and password in order to have financial gains. The rationale behind this is that with stolen credentials they can perform transactions as if they are done by original user. With credentials in place, hackers need not to spend time to compromise machines as they can just login. In 2013, there were 422

cases in which stolen passwords are involved. In the same fashion 144 downloader malware cases, 149 spyware, 152 command and control related, 165 backdoor malware, 223 RAM scrapping, 245 phishing, and 327 data-stealing malware cases were found. DBIR this year showed increased scope of security incidents that came from 50 organizations and 95 countries across the globe that include Latin American CERTs, Poland CERT, and US Secret Service [33].

The DBIR showed totally 1367 data breaches in 2013 which reflects an increase by 621 cases when compared to its previous year. However, the total number security incident is 63,437 in 95 countries. Out of them most of the security incidents are tied to nigh attack methods. There were many reasons for security risks. Some of them include sending an email to wrong person, payment card skimmers, Point of Sale (POS) intrusions, cyber espionage, Denial of Service (DoS) attacks, web application attacks, physical theft, privilege misuse, and crimeware. From the analysis of security incidents it is found that as many as 75% of them are in financial industry and in the form of payment card skimming, DDoS attacks and web application attacks. Around 54% of the security incidents are in manufacturing industry due to DDoS and cyber espionage. Many security incidents are result of DDoS (33%) and POS system hacking (31%) besides card skimming and stolen security credentials.

The report also observed that POS attacks are decreasing. In 2013, they were 198 including data theft. RAM scraping malware were increased in 2013 same as that of remote access connections and brute-force attacks. Web application attacks are 40% while POS attacks are 20%. In the same fashion, POS intrusions are reducing for many years. In 2013, RAM scraping malware was used for attacking POS systems. Hospitality industry in 2013 suffered from POS attacks with 75% of security incidents. Afterwards, the retail industry suffering from 31% of POS and 33% of DDoS attacks respectively. The report also revealed that attackers are becoming more innovative and efficient. In other words, attackers are learning new things much faster than other people.

7. POPULAR TRENDS IN DATA BREACHES

There are different kinds of data breaches. They are known a theft, unauthorized access to sensitive data, loss of data, combination, hacking or IT incident, improper dissemination of security information, others and unknown reasons.

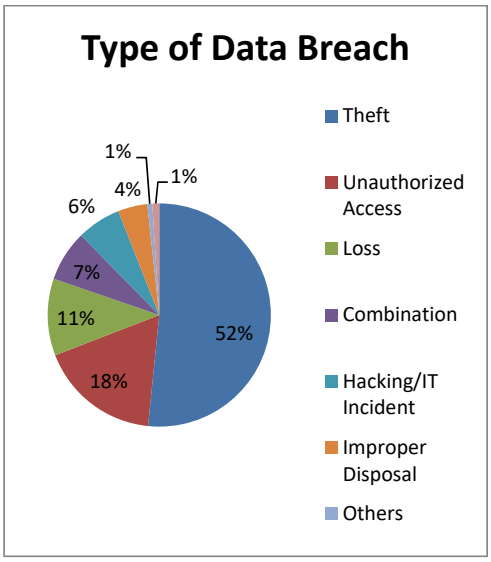

Figure 1: Different types of data breaches

As shown in Figure 1, it is evident that the information theft causes highest number of security breaches. As discussed earlier, stolen passwords also come into this category. It is 51% out of all breaches caused. Next to this is unauthorized access to sensitive data which is worth 17.3%. The combination attacks are of 7.3%, hacking or IT incidents are at 6.3% and 4.2% due to improper dissemination of data [36]. There are reports related to the USA where with respect to annual number of data breaches. Figure 2 shows the development of cyber attacks over a period of time. It shows the data breaches occurred between 2005 and 2014. The number of data breach incidents in the USA in 2014 is 783 and the number of records exposed is 85.61 million records.

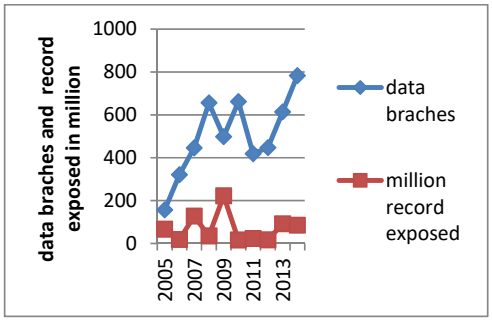

Figure 2: History of data breaches in the USA

Data breaches are more in the year 2014. The highest is 783 in 2014 and the least is 157 in 2005. The highest number of records exposed has occurred in the year 2009. It was 222.5 million records exposed and 498 incidents were identified. The number of records exposed in the year 2014 is 85.1 millions. The lease number of records exposed is 16.2 millions in the year 2010. The overall trend in the number of data breach incidents has increased gradually since 2005. It reveals that there is still the risk of data breaches and needs to be addressed [37]. In the presence of cloud computing it is more alarming as without security considerations, people do not inclined to outsource their data to public cloud.

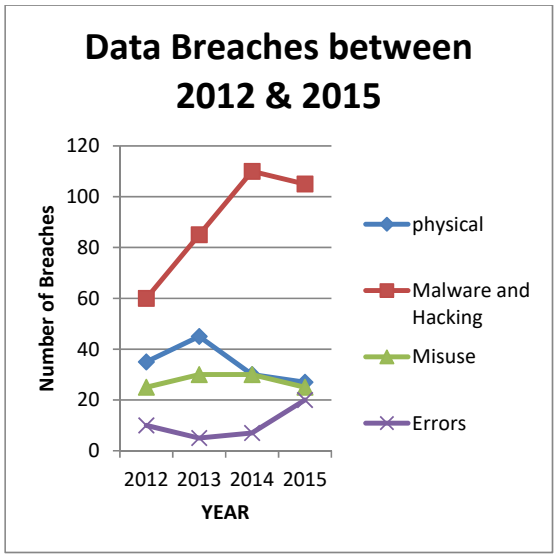

Figure 3: Data breaches between 2012 and 2015

As presented in Figure 3, it is evident that the trends in data breaches from 2012 to 2015 are provided. Number of breaches of malware and hacking is highest in all the years. Next to that is the breaches caused by human errors. Misuse of data related breaches are greater than human errors. The least number of breaches are caused by human errors consistently cross all the years. The results of this research reveal the importance taking measures to avoid data breaches especially that are caused by malware and hacking [38]. Figure 4 shows industry wide data breaches between 2012 and 2015.

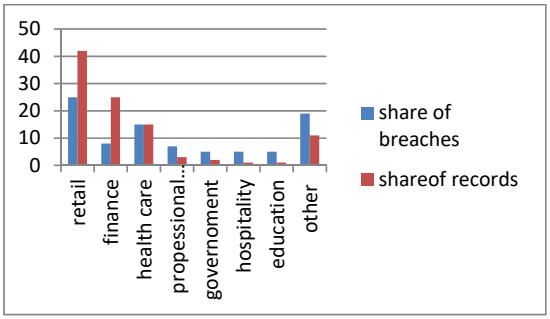

Figure 4: Industry wide number of data breaches and records breached between 2012 and 2015

Industry wide observations are made on number of data breaches between 2012 and 2015. Different sectors that are subjected to data breaches include retail, finance, healthcare, professional services, government, hospitality, education and others. The share of breaches and the share of records are provided. Highest share of breaches is with retail sector while the least goes to education sector. In the same fashion, the highest share of records goes to retail sector while the lease number of breaches share goes to education [39].

8. DIFFERENT WAYS TO AVOID DATA BREACHES

There are different ways in which data breeches can be avoided. Out of all, the first one is to bring awareness among end users. Unless it is done, other security measures are insufficient. The second way is to craft an encryption polity and enforce it to have data encrypted and the stolen data is not useful to adversaries. In many systems, it is important to have intrusion detection systems. This is the third way in which a data breach incident can be prevented. Since intrusion detection systems provide basic means of security to a system, they are right choice for preventing data breaches. The fourth way to avoid data breaches are to stop drive by downloads so as to avoid potential threats. The firth one is to have vulnerability assessment programs and use them frequently. The sixth one is that for all security software, it is important to update patches regularly as they are made available. Insider behaviour monitoring and taking regular backup are other two ways that can help in avoiding data breaches [7].

9. PROPOSED KEY MANAGEMENT FOR MITIGATING DATA BREACHES

Both symmetric and asymmetric cryptographic algorithms are used for effectiveness and efficiency. AES is the symmetric key (secret key) cryptography used for secure data transfer. RSA is the asymmetric key (public key) cryptography used for secure key transfer.

Notation	Description
ID_A	Id of node A
ID_B	Id of node B
$RN_1, RN_2, RN_3,$	Random numbers
Pub_{MA}	Public key of Authority
Pub_A	Public key of node A
Pub_B	Public key of node A
$\{M\}K_{AB}$	Shared key

Table 1: Notations used in the proposed scheme

Digital certificate is used to maintain unique identity to parties involved. One way hash function is used for integrity checking. Table 1 shows the notation used in the proposed key management system.

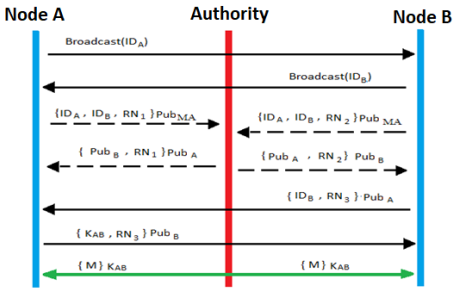

Figure 5: Proposed key management scheme for mitigating data breaches

As shown in Figure 5, the proposed security scheme has three parties involved. They are sender, receiver and authority. For secure key sharing, Node A broadcasts its id to node B. similarly Node B also broadcasts its id to node B. Node A send request with its id , node B id and with random number ($\{ ID_A, ID_B, RN_1\}Pub_{MA)}$ to Authority to get public key of node B for encryption. Node B also does like that. Authority provides public keys with same random number ($\{Pub_B, RN_1\}Pub_{A)}$and sent to relevant destination. Using that public keys node A and node B sent data with random number. After that node A and node B shares Secret key $\{M\}K_{AB}$. This key sharing is secure as there will not be manual key sharing. The propose scheme generates key to be used for decryption therefore it avoids vulnerability.

10. EXPERIMENTAL RESULTS

This section provides results of experiments with the proposed key sharing method which makes secure communication among parties. The results are observed in terms of communication overhead, memory usage and the rate of compromised keys.

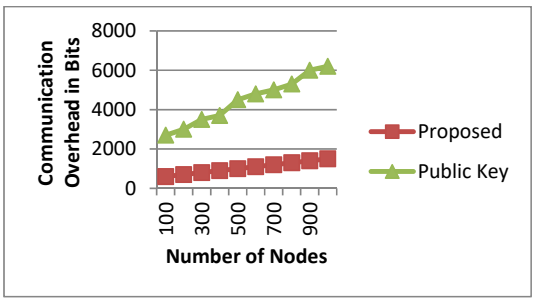

Figure 6: Comparison of Communication Overhead against number of nodes

The above figure differentiates between communications overhead against number of nodes with proposed and public key methods. It clearly shows that proposed method performs better than existing.

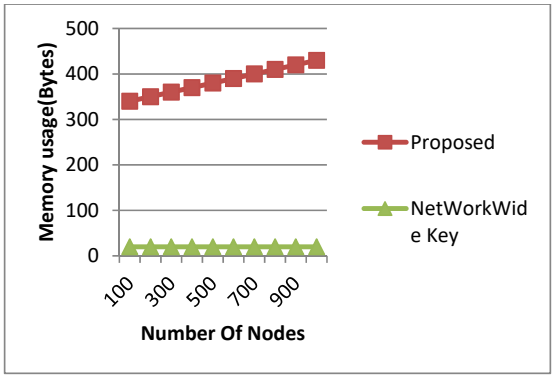

Figure 7: Comparison of memory usage against number of nodes

The above figure differentiates Comparison of memory usage and number of nodes with proposed and public key methods. It clearly shows that proposed method performs better results than Network wide key approach.

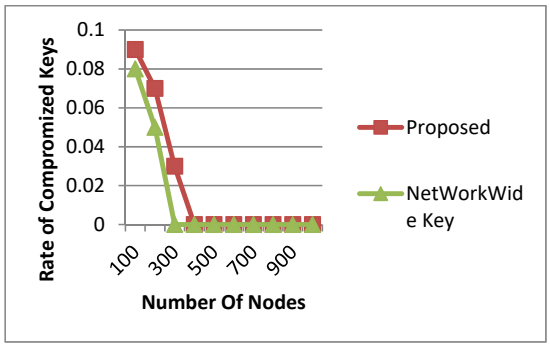

Figure 8: Comparison of rate of compromised keys with number of nodes

The above figure differentiate between Comparison of rate of compromised keys and number of nodes with proposed and network wide key methods .It clearly shows that proposed method performs better results than Network wide key. Thus it is understood that the proposed methodology can be used to have cryptographic solution for avoiding data breaches. When cryptography is in place, the adversaries though they steal data it will not make any sense to them. That is the power of cryptographic solution. However, it is not comprehensive in nature to cover all kinds of data breeches. Therefore further research is needed to have a comprehensive approach to prevent data breaches.

11. CONCLUSIONS AND FUTURE WORK

In this paper we presented the insights found from the literature related to data breaches in cloud computing. The data breaches were for many reasons such as malware, human errors, theft, loss of sensitive data, unauthorized access, hacking, improper dissemination of security credentials, and so on. It is found that the role of stolen passwords is more on the data breaches when compared to any other causes of data breach. Theft is one of the causes of data breaches which is of 51%. Therefore it is important to keep private and confidential information secret and avoid theft of data. Since 2005 data breaches have been observed in increasing trend in the USA. According to a report, data breaches caused by malware and hacking are more between 2012 and 2015. The share of breaches and share of records in million are more in retail market when different industries are studied. In this paper we proposed a methodology for protecting cloud data from data breaches. It is based on cryptography meant for mitigating data breaches in cloud computing. Our experimental results are evaluated in terms of communication overhead, memory usage and rate of compromised keys. The proposed scheme showed better performance when compared with other state of the art scheme for encryption to prevent data breaches. In our future work, we consider other means of preventing data breaches and propose a comprehensive framework that targets all the kinds of data breaches.

REFERENCES

[1] Chirag Modi , Dhiren Patel , Bhavesh Borisaniya , Avi Patel and Muttukrishnan Rajarajan. (2013). A Survey on Security Issues and Solutions at Different Layers of Cloud Computing. City Research Online, P1-31 .

[2] Chimere Barron, Huiming Yu and Justin Zhan . (2013). Cloud Computing Security Case Studies and Research . Proceedings of the World Congress on Engineering. II, P1-5 .

[3] Dimitrios Zissis and Dimitrios Lekkas. (2012). Addressing cloud computing security issues. elsever, p583–592.

[4] Te-Shun Chou. (2013). SECURITY THREATS ON CLOUD COMPUTING VULNERABILITIES . International Journal of Computer Science & Information Technology. 5 (3), p79-88.

[5] Nathalie Brender and Iliya Markov . (2013). Risk perception and risk management in cloud computing: Results from a case study of Swiss companies. international Journal of information Management. 33 (5), p1-17 .

[6] Muhammad Kazim and Shao Ying Zhu. (2015). A survey on top security threats in cloud computing. International Journal of Advanced Computer Science and Applications. 6 (3), P1-6 .

[7] Perimeter. (2010). 8 Ways to Prevent Data Breaches - Slide 8.Available: https://www.itbusinessedge.com/slideshows/show.aspx?c=79585&slide=8. Last accessed Jan 10, 2018.

[8] George Yee. (2012). Privacy and Security for Cloud Computing. Springer, P1-312.

[9] Issa M. Khalil and Abdallah Khreishah . (2013). Security Concerns in Cloud Computing . IEEE, p411-416.

[10] Ms. Disha H. Parekh and Dr. R. Sridaran. (2013). An Analysis of Security Challenges in Cloud Computing. International Journal of Advanced

Computer Science and Applications. 4 (1), p38-46 .

[11] Vahid Ashktorab and Seyed Reza Taghizadeh. (2012). Security Threats and Countermeasures in Cloud Computing. International Journal of Application or Innovation in Engineering & Management . 1 (2), p234-245.

[12] Younis A.Younis, Madjid Merabti and Kashif Kifayat. (2013). Secure Cloud Computing for Critical Infrastructure: A Surver, P1-7 .

[13] Diego Perez-Botero, Jakub Szefer and Ruby B. Lee. (2013). Characterizing Hypervisor Vulnerabilities in Cloud Computing Servers. ACM, p1-8.

[14] Rohit Bhadauria and Sugata Sanyal . (2012). Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques, p1-20 .

[15] Alice Hutchings, Russell G Smith and Lachlan James. (2013). Cloud computing for small business, Criminal and security threats and prevention measures, (456), p1-8.

[16] Alessio Botta , Walter de Donato, Valerio Persico and Antonio Pescapé. (2016). Integration of Cloud computing and Internet of Things, A survey. elsever, p684–700.

[17] Ahmad Rashidi and Naser Movahhedinia . (2012). A Model for User Trust in Cloud Computing. International Journal on Cloud Computing, Services and Architecture. 2 (2), p1-8.

[18] Monjur Ahmed and Mohammad Ashraf Hossain. (2014). CLOUD COMPUTING AND SECURITY ISSUES IN THE CLOUD. International Journal of Network Security & Its Applications. 6 (1), p25-36 .

[19] Mouna Jouini, Anis Ben Aissa, Latifa Ben Arfa Rabai and Ali Mili. (2012). Towards quantitative measures of Information Security, A Cloud Computing case study . International Journal of Cyber-Security and Digital Forensics, p248-262.

[20] Mazhar Ali a,c, Samee U. Khan a and Athanasios V. Vasilakos. (2015). Security in cloud computing, Opportunities and challenges. elsever, p357–383.

[21] Mr. G. Nanda Kishor Kumar and Mr. M. Naresh. (2017). SECURITY THREATS IN CLOUD COMPUTING. International Journal of Application or Innovation in Engineering & Management, p983 -992.

[22] Ikechukwu Nwobodo, Hossein Jahankhani and Aloysius Edoh . (2014). Security challenges in the distributed cloud computing . International Journal of Electronic Security and Digital Forensics. 5 (1), p39-51 .

[23] Jay P. Kesan, Carol M. Hayes Masooda and N. Bashir. (2013). Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency. Washington and Lee Law Review. 70 (1), p341-472 .

[24] Pradeep Kumar Tiwari and Dr. Bharat Mishra. (2012). Cloud Computing Security Issues, Challenges and Solution. International Journal of Emerging Technology and Advanced Engineering. 2 (8), p306-310.

[25] Lee Badger, Robert Bohn, Shilong Chu, Mike Hogan, Fang Liu, Viktor Kaufmann, Jian Mao, John Messina, Kevin Mills, Annie Sokol, Jin Tong, Fred Whiteside and Dawn Leaf. (2011). US Government Cloud Computing Technology Roadmap. NIST Cloud Computing Program Information Technology Laboratory. 1, p1-85 .

[26] Seyyed Mohsen Hashemi and Mohammad Reza Mollahoseini Ardakani . (2012). Taxonomy of the Security Aspects of Cloud Computing Systems-A Survey . International Journal of Applied Information Systems. 4 (1), p1-8.

[27] Carlo Marcelo Revoredo da Silva, José Lutiano Costa da Silva, Ricardo Batista Rodrigues, Leandro Marques do Nascimento and Vinicius Cardoso Garcia . (2013). Systematic Mapping Study On Security Threats in Cloud Computing . International Journal of Computer Science and Information Security. 11 (3), P1-10.

[28] Sultan Aldossary and William Allen. (2016). Data Security, Privacy, Availability and Integrity in Cloud Computing, Issues and Current Solutions. International Journal of Advanced Computer Science and Applications. 7 (4), p485 -498.

[29] Te-Shun Chou. (2013). SECURITY THREATS ON CLOUD COMPUTING VULNERABILITIES . International Journal of Computer Science & Information Technology. 5 (3), p79-88.

[30] Kashif Munir and Prof Dr. Sellapan Palaniappan. (2013). FRAMEWORK FOR SECURE CLOUD COMPUTING. International Journal on Cloud Computing, Services and Architecture. 3 (2), p21-35.

[31] James Sanders. (2014). Dropbox and Box leak files in security through obscurity nightmare. Available: http://www.techrepublic.com/article/dropbox-and-box-leak-files-in-security-through-obscurity-nightmare/. Last accessed May 8, 2014.

[32] Sekhar Sarukkai. (2015). Anthem's Breach and the Ubiquity of Compromised Credentials. Available: https://blog.cloudsecurityalliance.org/2015/02/09/not-alone-92-companies-share-anthems-vulnerability/. Last accessed February 9, 2015

[33] Kelly jack higgins. (2014). Stolen Passwords Used In Most Data Breaches. Available: http://www.darkreading.com/stolen-passwords-used-in-most-data-breaches/d/d-id/1204615. Last accessed 22th april 2014.

[34] Thomas Fox-Brewster. (2015). Anti-Virus Firm BitDefender Admits Breach, Hacker Claims Stolen Passwords Are Unencrypted. Available: http://www.forbes.com/sites/thomasbrewster/2015/07/31/bitdefender-hacked/. Last accessed Jul 31, 2015.

[35] Samuel Gibbs. (2015). TalkTalk criticised for poor security and handling of hack attack . Available: http://www.theguardian.com/technology/2015/oct/23/talktalk-criticised-for-poor-security-and-handling-of-hack-attack. Last accessed 23 Oct 2015.

[36] Top 5 Security Risks (2013). TOP 5 HIPAA SECURITY RISKS AS PROVIDERS MIGRATE TO THE CLOUD. Available: https://cloudtweaks.com/2013/05/top-5-hipaa-security-risks-as-providers-migrate-to-tthe-cloud/. Last accessed May 1, 2013.

[37] Nate Lord . (2018). THE HISTORY OF DATA BREACHES.

[38] Rohit Gupta. (2016). Data Breaches in Cloud-Based Enterprises.Available: https://blogs.oracle.com/oraclesecurity/data-breaches-in-cloud-based-enterprises. Last accessed April 13.

[39] Rohit Gupta. (2016). Data Breaches in Cloud-Based Enterprises.Available: https://blogs.oracle.com/oraclesecurity/data-breaches-in-cloud-based-enterprises. Last accessed April 13.

[40] Rick Robinson. (2014). The Impact of a Data Breach Can Be Minimized Through Encryption. Available: https://securityintelligence.com/the-impact-of-a-data-breach-can-be-minimized-through-encryption/. Last accessed October 21, 2018.