Log-Based Approach for Security Implementation in Cloud CRM's

Madhur Patidar and Pratosh Bansal

1 Introduction

Customers are one of the most valuable assets for an organization. As a result, dependency on customers for an organization and developing customer's trust becomes a key issue for a company's business process. Not only retaining the existing customers but attracting new customers is also vital. So understanding the customer's needs and customer satisfaction plays a crucial role. Hence, for increasing customer's lifetime value with the organization and improving business processes, a proper understanding of the current business trends and keeping a track of customers association with an organization acts as an important metric.

E-commerce is a similar process that deals with buying and selling of products, wherein the transactions are performed through the web which comprises many categories such as B2B, B2C, C2B, C2C, etc. Business-to-Consumer (B2C) is an important part of e-commerce, wherein the consumer is the final customer. Several techniques are developed so that the shoppers turn into buyers efficiently for an organization. B2C marketing has evolved over the time on account of knowing the audience in a better way, analyzing the online contents generated by users, building brand loyalty, etc. Also, these involving best practices for the promotion of products and services have many CRM solutions built for them.

Customer Relationship Management (CRM) plays a vital role when it comes to keeping track of a company's interactions with its customers and activities such as emails, website accessed, etc. It is mainly used for providing better services to the customers and helps the sales teams to work effectively and focused. One of the main benefits of CRM applications is that data from heterogeneous departments are

M. Patidar (✉) · P. Bansal
Department of Information Technology, IET, Devi Ahilya Vishwavidyalaya, Indore, MP, India
e-mail: madhurpatidar15@gmail.com

P. Bansal
e-mail: pratosh@hotmail.com

R. K. Shukla et al. (eds.), *Data, Engineering and Applications*,
https://doi.org/10.1007/978-981-13-6351-1_4

stored centrally and can be accessed anytime whenever required. Improved relationships with the existing clients help ensure better sales, identification of customer requirements in an effective and planned manner, and also determining which of the customers are profitable. Satisfaction of customers is focused upon largely. CRM applications have been one of the crucial factors for an organization's motivation toward moving over cloud and one of the leading application hosting investments [1].

Cloud-based CRM's are becoming increasingly popular today on account of several benefits over the traditional CRM's as discussed in Sect. 3.1 ahead. Being a cloud application, these are also susceptible to attacks and other security concerns as discussed in Sect. 3.2 ahead. We followed a log-based approach to overcome and minimize these concerns as discussed in Sect. 4 ahead.

The motive behind this paper is to identify certain loopholes with respect to security and privacy over the cloud-based CRM solutions and to design a system that monitors and alerts such undesired issues through a proper log management mechanism.

The paper is structured as follows. The current section gives a brief overview of the paper. The next section subsequently deals with the literature review followed by significance of cloud CRM's in enterprises, the security concerns associated, logs' overview, and approaches for log management. The next section includes the methodology and outcomes followed by the conclusion and future work at the end.

2 Literature Review

Works related to identifying security concerns in cloud-based CRM applications and approaches to minimize them have been proposed by various authors. Huei Lee, Kuo Lane Chen, Chen-Chi Shing, and Marn-Ling Shing highlight the security concerns with cloud CRM's in their papers [2]. S. Xiao and Genguo Cheng gave a research based on cloud CRM's [3]. Rajiv R. Bhandari and Nitin Mishra focused on cloud implications in context to CRM applications and implementation of auditing techniques to achieve the level of security in cloud-based applications. At the end, the author also mentions the significance of log management in cloud-based enterprise applications such as CRM's [4]. Raffael Marty in his paper considered log as an important metric for forensic purposes. The author further highlights the necessity for log management in the cloud applications and elaborates various kinds of log records [5]. Mahdi Seify emphasized security through risk management for cloud CRM solutions [6]. Julia Vuong and Simone Braun provided a secured design-based solution for ensuring security for multi-tenant cloud CRM's. Also, the authors provided security algorithms for encryption that focuses on optimizing the performance of the system [7]. Miguel Rodel Felipe, Khin Mi Mi Aung, Xia Ye, and Wen Yonggang proposed a cloud CRM model which is based on full homomorphic encryption of database to provide a secured solution [8]. M. Vanitha and C. Kavitha emphasized secured encryption algorithms for encrypting data at the client and the network ends,

helpful for enterprise applications such as CRM's dealing with lots of transactional data [9].

So by studying the above research papers, we inferred that the authors identified the main problems with cloud CRM's as the security concerns which may compromise the sensitive data stored of the users. Also, by the authors' review over the importance of log management in cloud-based enterprise applications, we got a motivation toward adopting a log-based approach for eliminating the security issues concerned with cloud CRM's.

3 Research Background

3.1 Significance of Cloud CRM's

CRM's can be traditional also known as on-premise or it can be hosted on cloud. These are the two broad categorizations for CRM's.

Traditional CRM's refer to those where the management is done by the in-house IT department with the organization's control over the data. CRM, being sales driven, is based on direct feedback from the customers and is often automated. Although the flexibility for customization is more here, these CRM's usually have higher upfront costs. Also, it is time-consuming in fully integrating it into the business environment of client. So, these are suitable for businesses with more complex needs and technical expertise. Hence, due to its high maintenance and costs, alternative CRM's such as cloud-based CRM's are increasingly becoming popular [10].

Cloud-based solutions provide better services on account of benefits such as IT cost savings, reliability, scalability, availability, and disaster recovery features which ensures business continuity. The management is being looked upon by the service providers, and the SLA conditions lead to a proper delivery and maintenance of the services. Hence, the flexibility provided by cloud solutions encourages more and more business organizations to adopt the same.

Following are some of the statistics which proves that enterprises will adapt cloud-based solutions at a rapid pace in near future.

- By 2018, cloud-based platforms will host more than half of the infrastructure of more than 60% of enterprises [11].
- By 2019, cloud apps will be a part of 90% of the total mobile data traffic which will subsequently be attaining 60% compound annual growth rate (CAGR) [11].

The use of cloud CRM's is increasing day by day, wherein the services are provided through a remote-based location. CRM applications based on cloud have a significant proportion among other cloud applications as per the CSA Survey Report 2016 as shown in Fig. 1.

Some of the key benefits of cloud CRM's can be summarized below:

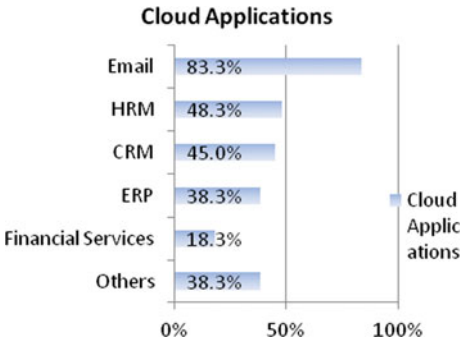

Fig. 1 Cloud applications' ratio as per CSA survey report 2016

- Based on real-time and updated data of the customers, it saves time involved for uploading, backup, and maintenance purposes.
- Data analysis process became faster and smoother as keeping track of business emails, user's activities including the mails forwarded, and other interactions have greatly enhanced.
- Integration of cloud CRM with big data platforms, which being cloud-friendly, helps in processing huge volumes of data.
- Synchronization with mobile and tablet devices helps in better functioning.
- Focuses on a proper training of the employees by offering free trials for the solutions, documentations, and ongoing support.
- Better organization of data, integration of data from multiple sources, and proper visualization of data which helps in faster decision-making process.
- Cost reduction is one of the main factors as cloud CRM's are based on subscription, thereby eliminating hardware and license purchase costs, installation and maintenance processes, etc.
- Being accessible from anywhere and at any time and with use of additional features such as mobile apps, it increases employee productivity and hence the business growth and optimization.
- Features such as easy deployment help cloud CRM solutions as a preferred one for the small- and medium-sized businesses even with small expertise in technology.

IT environment is greatly affected by the increased adoption of social, mobile, analytics, and cloud (or SMAC). Preference for Software as a Service (or SaaS) by ERP and CRM software companies like Oracle Corp. (ORCL), IBM Corp. (IBM), and Microsoft Corp. (MSFT) forces them to invest billions of dollars in cloud-related products, solutions, and initiatives. Several cloud CRM solutions are available in market today. Salesforce.com is the most popular among them. Figure 2 shows popular cloud CRM vendors.

Hence, we can say that there is a great requirement for maintaining the data associated with cloud CRM's as more and more organizations are getting associated with the same. But, on the other hand, there are some risk factors involved too as discussed in the next section.

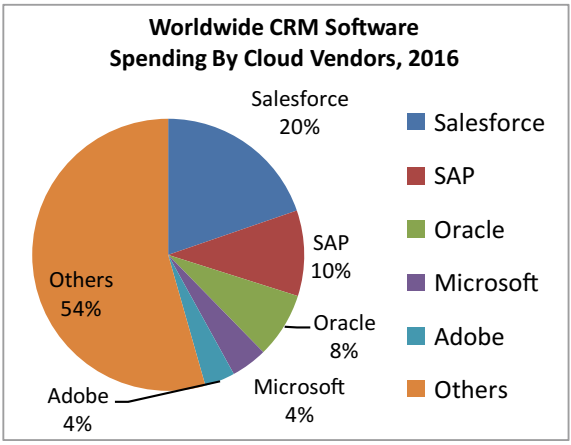

Fig. 2 Cloud CRM software vendors with their proportion in market [12]

3.2 Security Concerns in Cloud CRM's

Security of data is one of the major concerns as far as storing data on the cloud is concerned. CRM applications are no exception to it. Multiple CRM records are maintained by the service providers. So authorization, safety, and access control of CRM data are of utmost importance for an organization. Data breaches can have unpredictable effects on an organization. Today, for various advertising purposes, personal data of customers is being taken through the social media. A single instance for a cloud CRM contains large amount of confidential and proprietary details regarding the customer. Hence, data privacy issues are vital for both corporate and the consumer. Although CRM vendors try to provide measures for safeguarding our data, still vulnerability of data leakage cannot be fully stopped, hence, giving rise to frauds and cybercrimes too.

There are number of security concerns possible with the data stored over cloud CRM's. Some of the main concerns include:

- **Improper activities at network, client, and server ends**: This includes any vulnerable and abnormal activities observed, e.g., servers being compromised, change in the host activities or any other manipulations over the network end, bulky traffic and multiple packets over the network, intrusion attempts, machines not responding, etc.
- **Downtime/outages**: Even short and infrequent CRM outages can affect business to a great level incurring huge losses.
- **DDOS attacks**: These are the attacks that cause the cloud services to be disrupted, thus making it inaccessible. The targeted components may be network bandwidth, disk storage, RAM, etc.
- **Malware attacks**: Security mechanisms must be implemented in order to avoid malicious intends and to save the systems from halts, loss of data, damages caused to the hardware components and the software or the applications, any system inop-

erability issues, etc. An example of such attack is **Zeus Trojan** that has been known to be spotted on Salesforce.com, the leading CRM solutions provider in the world. The malware's main purpose was to gather sensitive business data [13]. Similarly, variant known as **Dyre** or **Dyreza** has been known to target Salesforce.com.

- **Data breaches**: Data stored on cloud CRM's is vulnerable to breaches if the proper designing of databases is not done. Users' data can be targeted for attacks even if there may be flaw in any one of the client's applications. As a result, other client's data may also get exposed. As the users no longer have control over their data, so any of the cryptographic techniques to protect the integrity of their data proves ineffective.
- **Data-in-flight**: The data that is being transmitted is susceptible to cyberattacks, risks of being transmitted to wrong locations, etc. A strong encryption mechanism needs to be applied to protect the sensitive data along its motion.
- **Masquerade attacks**: These are the attacks that focus mainly on obtaining personal data by misusing an individual's identity. The attackers, by taking into trust the customers through false image of a company's representative, can actually sell data to other parties which can further use it for identity theft purposes.
- **Service providers' dependencies**: The users are not sure how is their data being managed by the service provider. As the data can be sensitive and private, issues concern the security of the same arises.
- **Improper designing of SLA's**: Policies regarding deleting the traces of data after the contract, planned maintenances from downtimes, backups, and disaster recoveries might not be properly formulated in the SLA's.

Looking at these attacks, we can infer that people cannot rely exclusively on their SaaS providers for securing data inside their CRM applications.

3.3 Logs in Cloud CRM's

Logs refer to the events or activities by users and entities within the networks of the system. Being an important aspect of analytical data, logs are very useful to monitor business processes and faults in infrastructural components and applications. Log records help in identifying error conditions, unauthorized access of resources, patterns of user behavior, incidents alerting, any nonprivileged access, etc. Presently, for collection of logs over cloud CRM's for any forensic investigations, there are some cloud simulation tools available which eliminate dependency on the CSP. Examples of some simulators include CloudSim, Cloud Analyst, Green Cloud, etc. Evaluation and monitoring of logs are very important in context to cloud forensic investigations as privacy of customers' information is directly linked with the business and financial perspectives of an organization [14].

3.4 Log Management Approaches

Several approaches helpful in managing logs have been proposed to effectively minimize security concerns over cloud CRM's. Some of the useful approaches are as follows:

- **SIEM**—It refers to security information and event management. This includes user activities monitoring, using log correlation to track malicious events, aggregation of log data, real-time analysis of alerts generated by applications, analysis of log files, reporting through dashboards, etc. [15].
- **SANS logs' reports**—This includes some critical log reports that help in determining the techniques to be followed for log management, e.g., authentication and authorization report which includes login failures and successes by users, suspicious network traffic patterns, etc. [16].
- **SOC**—It refers to security operations center where the main focus is upon detecting, analyzing, and responding to cyber incidents through 24/7 monitoring processes by analyzing the activities across networks, servers, and databases of an organization.

4 Proposed Methodology

Enterprise data comprising of customers records, business records, chats, emails, phone records and tracks, last sales records, timestamps, and past records act as an important source for security and IT operations and therefore motivates us for a systematic log management process.

In order to maintain the security principles, the following methods are being focused upon by us:

- **Log monitoring process**: A continuous monitoring process of generated logs in order to detect any suspicious or malicious threats over the privacy and security of data report the same through dashboards (identifying abnormal activities not adhering to standard patterns). To keep a track of the packet flow, web-based activities, the type of request by the client, IP of client, date/time, browser type, and other recorded instances at the server from the requests sent through the browser. For achieving the same, we will follow the approaches as mentioned in Sect. 3.4.
- **Predictive analysis through alerting**: Reporting of security issues analyzed through log monitoring by a well-defined automation of events or alerts.
- **Log mining and aggregation techniques**: Log management measures include data aggregation from various sources such as servers, networks, databases, etc.
- **Post-attack identifications/Forensic analysis**: In case of any suspicious attempts for security breaches, analyzing the causes of attacks through the symptoms observed will help us in preparing and safeguarding our systems from attacks in future.

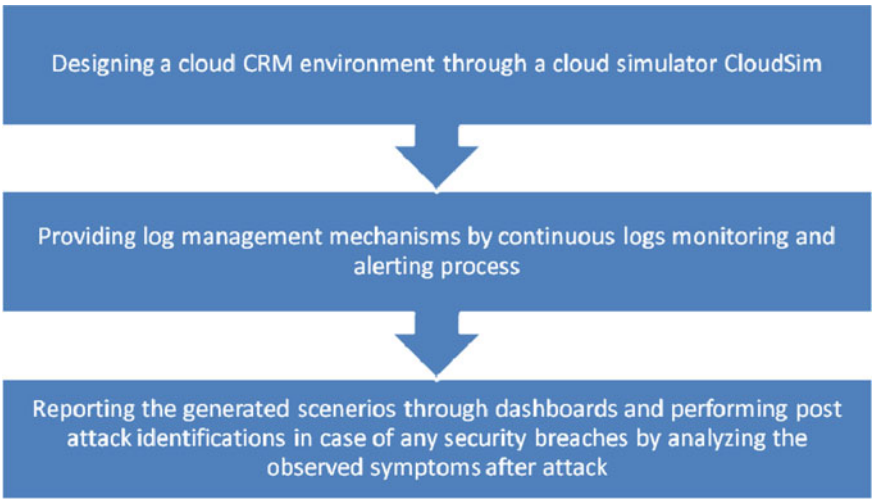

Fig. 3 Proposed methodology

- **Appropriate troubleshooting**: Based on the log analysis and forensic procedures applied, it will be easier to identify and solve the potential faults and other flaws in the application.
- **Fault tolerance techniques**: In order to ensure 24 * 7 business operations or business continuity, strategies such as backups and fault tolerance techniques to be focused upon are covered here.

The work also focuses on the following concerns with respect to log management.

- Log centralization.
- Log integrity preservation.
- Log records retention and maintenance.

The methodology followed is as shown in Fig. 3 and focuses on analyzing different instances of the log records such as timestamps, logged in user entries, browser used, IP addresses used, reasons for access denials, etc. To achieve the same, we use a cloud simulator CloudSim for creating a cloud environment and generating the logs as shown in Fig. 4.

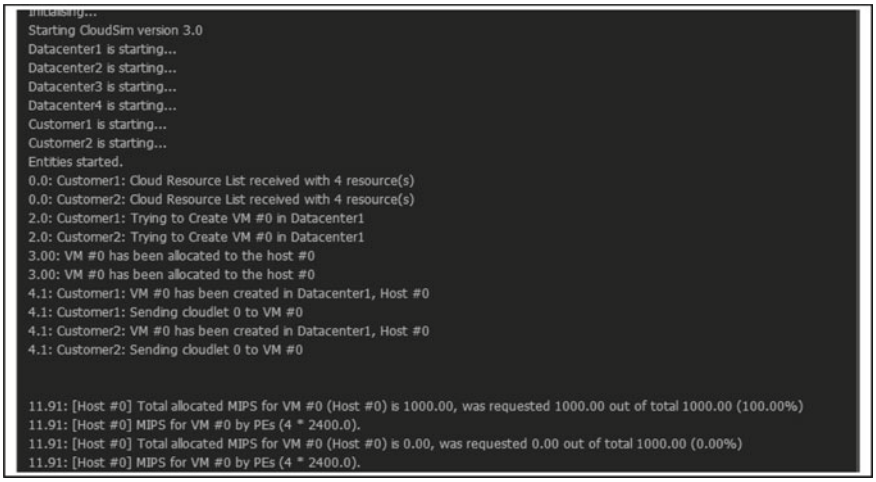

Fig. 4 Log generation through cloud simulator

5 Proposed Outcomes

The resulting outcome will mainly help in retaining the security principles and business continuity aspects with respect to cloud-based CRM firms, and hence will help in achieving the following:

- The faster recovery and troubleshooting processes along with the 24 * 7 continued business operations will help in maintaining a smooth relationship of a company with its customers.
- Log analyses from different domains such as application, network, and interface are quite useful.
- A proper, secure, reliable, and prompt cloud service in combination with systematic log management generation process will result in a fast growth sector particularly for CRM and ERP applications.
- Faster data analysis through dashboards.
- Enhanced customer satisfaction for organizations on account of no issues concerning security and privacy regarding CRM-sensitive data.
- Systematic monitoring process to keep track of activities helps in assisting regarding logs' identification and analysis processes.
- Useful in all web-based domain areas such as organizations involving keeping a track of large number of customer records where customer trust regarding privacy of their data acts as a vital element.
- Useful for system administrators, security analysts, etc. where the job profiles require strict monitoring and auditing processes.
- Helpful in protecting the sensitive data stored in different governmental, commercial, and industrial organizations.

6 Conclusion

The rate of enterprises moving toward the cloud suggests the need for systematic security measures and for that purpose log management is a worthy of consideration. The paper provides a roadmap to provide a secured solution by maintaining logs for cloud-based CRM applications. This work mainly concentrates on monitoring and alerting process, troubleshooting, and forensic procedures in case of any abnormalities observed with context to cloud CRM's. The resulting outcomes are quite beneficial for organizations as discussed in Sect. 5.

7 Future Work

In future, we will be working to broaden the areas of the current project to cover majority of the areas of time cloud environments. The project can be further utilized for log management in case of large-scale organizations dealing and maintaining big data. Other works will include analyzing the results after performing live attacks, generation of large number of data sets, and working on the security requirements on the same and performing the results on live data centers used for server requirements.

References

1. Petkovic, I.: CRM in the cloud. In: 2010 8th International Symposium on Intelligent Systems and Informatics (SISY), pp. 365–370. IEEE (2010)
2. Lee, H., Chen, K.L., Shing, C.C., Shing, M.L.: Security issues in customer relationship management systems (crm). In: Decision Sciences Institute 37th Annual Conference Bricktown-Oklahoma City March, vol. 1 (2006)
3. Xiao, S.: Application research of CRM based on SaaS. In: 2010 International Conference on E-Business and E-Government (ICEE), pp. 3090–3092. IEEE (2010)
4. Bhandari, R.R., Mishra, N.: Encrypted IT auditing and log management on cloud computing. Int. J. Comput. Sci. Issues (IJCSI) **8**(5) (2011)
5. Marty, R.: Cloud application logging for forensics. In: Proceedings of the 2011 ACM Symposium on Applied Computing, pp. 178–184. ACM (2011)
6. Seify, M.: New method for risk management in CRM security management. In: Third International Conference on Information Technology: New Generations, 2006, ITNG 2006, pp. 440–445. IEEE (2006)
7. Vuong, J., Braun, S.: Towards efficient and secure data storage in multi-tenant cloud-based CRM solutions. In: 2015 IEEE/ACM 8th International Conference on Utility and Cloud Computing (UCC), pp. 612–617. IEEE (2015)
8. Felipe, M.R., Aung, K.M.M., Ye, X., Yonggang, W.: StealthyCRM: a secure cloud CRM system application that supports fully homomorphic database encryption. In: 2015 International Conference on Cloud Computing Research and Innovation (ICCCRI), pp. 97–105. IEEE (2015)
9. Vanitha, M., Kavitha, C.: Performance enhanced security for enterprise cloud application. In: 2016 International Conference on Computer Communication and Informatics (ICCCI), pp. 1–5. IEEE (2016)

10. Ghafarian, A.: Foreniscs analysis of cloud computing services. In: Science and Information Conference (SAI), 2015, pp. 1335–1339. IEEE (2015)
11. Columbus, L.: Roundup of cloud computing forecasts and market estimates Q3Update. http://www.forbes.com/sites/louiscolumbus/2015/09/27/roundup-of-cloud-computing-forecasts-and-market-estimates-q3-update-2015/#840e1b86c7ad (2015)
12. Stamford, C.: Gartner says customer relationship management software market grew 12.3 percent. http://www.gartner.com/newsroom/id/3329317
13. Osborne, C.: Zeus variant targets Salesforce.com accounts, SaaS applications. http://www.zdnet.com/article/zeus-variant-targets-salesforce-com-accounts-saas-applications
14. Shenk, J.: Log management in the cloud: a comparison of in-house versus cloud-based management of log data. A SANS Whitepaper, October (2008)
15. Balaji, N.: Security information and event management (SIEM)—a detailed explanation. https://gbhackers.com/security-information-and-event-management-siem-a-detailed-explanation/
16. The 6 categories of critical log information. https://www.sans.edu/cyber-research/security-laboratory/article/sixtoplogcategories