ISSN:0975-9646

Securing E-Mail System of Web Data Base Using Cloud Computing

Tejaswi.K, Sridevi.M, Vishnu Murthy.G
Department of Computer Science and Engineering
Anurag group of Institutions (Formerly CVSR College of Engineering)
Venkatapur(V), Ghatkesar(M), Andhra Pradesh, India

Abstract:- Web data base security is more than keeping unauthorized users out of your network and viruses off your desktops. It's not just about encrypting data or blocking spam, monitoring compliance, ensuring privacy or protecting company resources, important as all of those are. If you take the wider view, security means ensuring the confidentiality, integrity and availability of business information in side any web database. While line-of-business applications and back-end databases are crucial, more and more of that business information is in email on desktops and laptops, which makes it both convenient and vulnerable. It doesn't matter where in the value or supply chain you are, you're relying on email for all manner of vital communications.

Keywords: Security as a Service[1], Cloud computing, cloud security, Policy Management, Risk management[2].

I. INTRODUCTION

Cloud computing provides Internet-based services, computing, and storage for users in all markets including financial, healthcare, and government. This new approach to computing allows users to avoid upfront hardware and software investments, gain flexibility, collaborate with others, and take advantage of the sophisticated services that cloud providers offer. However, security is a huge concern for cloud users. Cloud services and virtualization are driving significant shifts in IT spending and deployments.

Cloud services give companies the flexibility to purchase infrastructure, applications, and services, from third-party providers with the goal of freeing up internal resources and recognizing cost savings. Virtualization allows maximum utilization of hardware and software, increasing cost savings, as well.

II. BENEFITS FOR THE CLOUD COMMUNITY

With the exponential increase in data deposited in cloud environments (both public and private), research in the area of data, information, and knowledge stored and processed in the cloud is timely. Data is stored in many different forms, and processed in a myriad of methods. There is a need for an authoritative voice in making sense of the key concerns with data storage and processing techniques. There is also an urgent requirement to align current practices with governance, risk and compliance regulations. Cloud providers have recognized the cloud security concern and are working hard to address it. In fact, cloud security is becoming a key differentiator and competitive edge between cloud providers. By applying the strongest security techniques and practices, cloud security may soon be raised far above the level that IT departments achieve using their own hardware and software. Before customers will entrust their IT needs to a cloud services they need two things: first, assurance that the cloud infrastructure is secureand compliant, and second, visibility into their own security and compliance in cloud or managed infrastructure.

Managed service and cloud providers have the technology and support they need to address these cloud computing security concerns. That means customers can move to the cloud with confidence. It also means you, as a provider, have the opportunity for unprecedented growth and market differentiation in this highly competitive space. So it is very important to develop a cloud service which possess highly secure. For that each cloud resource center has to fallow below strategy

A. Concept of Secure email –most of the web databases[3] are facing security problems with their E-mail services. Email is one of the main gateways into your business, and its security is a key requirement at all times. Regulatory requirements mean that a larger proportion of email now needs to be stored for many years, and you need to be sure that its integrity is preserved, and that full audit trails exist to show just who looked at a message, and where and when.at rest, in use and in motion is a key part of any IT security strategy and doing that in the cloud has significant advantages for confidentiality, integrity and availability. For one thing, you're protected from spam and malwarebefore it ever reaches your premises; keeping up with thousands of new threats a day is an unnecessary battle for individual businesses to fight.

For another, as with other cloud services you're gaining the expertise and economies of scale of a dedicated service, which means savings on up-front costs and ongoing administration, making a big difference to how quickly you can see value from the system you put in place.And for email in particular, having it protected in the cloud means it's available in the cloud; as convenient as having it on your laptop but without the security risks. That makes the difference between security that gets in the way of users, forcing them to resort to insecure workarounds to get their job done, and security that gives you the flexibility and control to allow business users to stay productive. At best, security is usually seen as a necessary evil; at worst it actually hampers the business. More than 80% of IT security

and business executives say they've given up opportunities for innovation in business because of concerns about information security.

B. Email intelligence [4]

You can give users access to a mass of useful information about customers, products, colleagues, negotiations, existing contracts and useful contacts, just by letting them search their email efficiently. Who is the best person to work with at a company you haven't dealt with recently? How quickly does a supplier usually get back to you? How often has a potential partner been recommended by colleagues? Often, theinformation they need is sitting in an old message, but if mail server quotas mean they only have a few weeks of email in their inbox then they're faced with losing access to key business information or keeping PST files on their hard drive, which exposes the information to a host of security threats and impedes E-Discovery should it be required. Making email available and searchable in the cloud means that it stays secure, but is stillaccessible. It's the best of both worlds for the user, the IT administrator and the business.

Users are no longer restricted by lack of resources, and can take advantage of being able to work anywhere, and at anytime.

C. Managing email security [5]:

Implementing on-premise infrastructure required to ensure an email system is secure and compliant takes time and requires significant post-installation maintenance. As the email attack surface is large, it's important for businesses to keep their security platform up to date – but this has significant time and budgetary impact, as well as affecting the resources available to IT departments. Time spent maintaining an email security system is time that's not being spent developing new systems or improving business processes. Putting security in place isn't a one-time deal. It also needs ongoing management, making sure any security infrastructure is kept up to date and regularly maintained. Mail administrators need to regularly patch and upgrade software to deal with new techniques employed by malware and spam authors. Significant investment will be required for hardware and software – which is an ongoing expense – as well as subscriptions to support services.

Appliance lifetimes are typically short, like PCs and servers, and they will need to be replaced every three or four years. Replacing appliances is another risk, as cover needs to be kept in place while new hardware is installed, and services are migrated between what are likely to be very different security platforms. The cost of an administrator's time needs to be taken into account too, as effective management of an email security platform will often require the equivalent of at least one, or maybe more, full-time positions. And beyond the individual costs, this is a permanently defensive approach to security, and one that means that mail security will always be a cost to a business, where it will be hard to identify any return on security investment. Getting and collating reports to help understand the returns is an issue in its own right, as fragmented servers and services make it hard to get the right level of visibility into the operations of your mail platform. Mail security teams will find it hard to report in terms ofbusiness benefits when the only effective metric is the number of days between security failures.

III. RISK MANAGEMENT AND SECURITY

And you can't simply ignore the problem because of the costs; effective email securityis a business necessity. Email introduces risks into the organization, and risks need to be managed. Insecure mail opens you up to all manner of attacks and issues. Spam gets in the way of normal mail traffic, and distracts staff.

Productivity drops every time a user has to delete a spam message, and with 80 – 85% of a user's email being spam, it's wasted time that quickly adds up. It's not just advertising spam, either. Spam is now one of the main routes malware takes into a company. A plausible message with an attachment is a ticking time bomb that could end up compromising machines, adding them to botnets and opening up their file systems tothe prying eyes of criminals. It's not just obviousspam that delivers malware; it can also comefrom trusted sources.

IV. FRAGMENTED SECURITY SYSTEMS

Once in place, an email security infrastructureis a key component of your business protection,mitigating risks and reducing exposure tothird-party threats. However it needs to be acoherent, easy-to-manage system. That's seldomthe case if you have a patchwork of systemseach that were put into place to answer specificthreats. Separate anti-virus tools sit next toanti-spam appliances, getting updates ondifferent schedules, while data loss preventiontools add to the complexity. Managing them allis another complex task, as they'll each havetheir own management tools, and systemadministrators will find themselves working witha mix of web user interfaces, remote desktops,and console applications. Making sure everythingis up to date becomes a full time task, not tomention testing rules and updated applicationsto ensure they don't affect your businessprocesses – an updated spam filter that stopscustomer emails from arriving is something noone wants.There's another problem that's exacerbated by the complexity of managing your own email security infrastructure: the window of vulnerability.

Email security is an arms race with spammers, phishers and malware authors – and they will often have the upper hand. Filters and signatures can only be updated after attacks have been identified and categorized, so you'll be left waiting for updates to be tested and installed hours or days after the bad guys have started using the loophole you're waiting to close. Fifty percent of systems are still un patched 60 days after patches are released – that's a long time to risk getting infected with malware.

High Risk Systems or data or virtual machines in cloud that if compromised (data viewed by unauthorized personnel, data corrupted, or data lost) would cause an extreme

disruption in the business, cause major legal or financial ramifications, or threaten the health and safety of a person. The targeted system or data requires significant effort to restore or the restoration process is disruptive to the business or other systems.

Next assign this risk level to each core network devices, distribution network devices, access network devices, network monitoring devices in cloud. If we implement the same thing at Network equipment such as switches, routers, DNS servers, and DHCP servers can allow further access into the network, and are therefore either medium or high risk devices. It is also possible that corruption of this equipment could cause the network itself to collapse. If we do so 80% problem is slaved.

Once you've assigned a risk level, it's necessary to identify the types of users of that cloud environment.

Admin of that cloud: responsible for internal users and network resources.

Internal users: It helps to provide limitation for local users while accessing cloud services.

Outside Partners External users with a need to access some resources.

Making security a service

Treating security as just a series of defenses doesn't give you much opportunity to differentiate your business. The place to add value and improve productivity is through what you enable with security.

Security in the cloud

You could outsource the management of your on-premise email infrastructure, but the problems (and costs) of the DIY security architecture remain. The alternative is to shift the burden of management off the IT department by moving it out of your network completely. This approach is often partially in place, with anti-spam facilities already outsourced to services that partly or wholly run in the cloud. Important as they are, anti-spam and anti-virus services are only part of the security story, especially in light of the current regulatory environment. Putting all your email security in the cloud will relieve your IT department of a considerable burden. There's no need to test patches, no need to wait for updates to install – and above all, little or no down time.

A well-designed security system needs to provide businesses with four key features:

• It needs to be available at all times, to the appropriate users.

• It needs to provide a business with the means to ensure the integrity of its systems.

• It needs to be confidential (making sure that only your company and partners can access mail and mail based processes).

• It needs to give you the means to control user actions.

Delivering all four is a complex task, and requires a mix of tools and technologiesmaking it well suited to a cloud service.

Anti-malware

No two anti-malware tools are identical. They all work differently, and they all update on different schedules. Some push out updates to their signature files every few minutes, with weekly or even daily updates to their engines. Others are slower, but offer a wider range of anti-virus features. It's important to use a mix of different anti-virus engines if you want to keep a network as secure as possible with as wide as possible coverage. If one engine is being updated, the others will still be working, and messages will continue to flow, but if you're doing this in house you'll need to find a way of staggering updates.

Building a suite of anti-malware tools takes time, as you need to continually monitor evolving threats and available technologies in the market. Another good reason to work with a cloud service is it can use its dedicated resources to ensure you always have the best in class anti-virus tools protecting your mail.

V. WEB APPLICATION FIREWALLS

Searching databases is usually done in the clear. And even if the query is encrypted, it has to be decrypted (revealing its contents) before it can be used by a search engine. What's worse is that databases themselves are stored as plaintext, Available to anyone gaining access. The smarter way to handle sensitive information would be to encrypt the queries, Encrypt the database and search it in its encrypted form. Even the industry-standard RSA encryption scheme—named after its inventors Rivest, Shamir and Adleman—is partially Homomorphic, in that it allows simple multiplication of two encrypted numbers to yield their product.

What Gentry andIBM have succeeded in crafting is a fully homomorphic encryption scheme where any mathematical operation can bemade to work as expected. Fully homomorphic encryption schemes theoretically allow cypher text to be manipulated aseasily as plaintext, making it perfect for modern cloud computing, where your data is located remotely. The HTTP protocol used in web database servers has been exploited by attackers in many ways, such as to place malicious software on the computer of someone browsing the web, or to fool a person into revealing private information that they might not have otherwise. Many of these exploits can be detected by specialized application firewalls called webdatabase application firewalls that reside in front of the web server.

These firewalls are a relatively new technology, as compared to other firewall technologies, and the type of threats that they mitigate are still changing frequently. Because they are put in front of web servers to prevent attacks on the server, they are often considered to be very different than traditional firewalls.as they are providing high security. Maintenance of this firewalls also a great challenge.

Hence in this paper we suggest a security as a service. In this concept a cloud environment will be established and this cloud environment will have this Web Application Firewalls. The organization which will ask for the security as a service the input and output network packets of that organizationwill be passing through this cloud environment.

If any application packet of this web database has the suspect as a malware or key logger they will be blocked at that cloud environment.Instead of mainlining multiple

firewalls for multiple webservers. We will have a single a secure cloud environment which will look after all these problems. Because of this secure cloud environment organizations will reduce their upkeep cost for the security management.

VI. POLICY MANAGEMENT IN CLOUD

While the public IT cloud has a silver lining for many adopters, it isn't without draw-backs, especially in regards to data protection. Once data has gone into a public cloud, data security and governance control is transferred in whole or part to the cloud provider. Yet cloud providers are not assuming responsibility, e.g. Amazon's web services contract states "we strive to keep your content secure, but cannot guarantee that we will be successful at doing so, given the nature of the internet". When handing over the data, the enterprise forfeits all control of the security of the data, unless they protect the data beforehand.

One of the best ways to leverage the cost and efficiency benefits of the cloud and virtualization while keeping sensitive information secure, is to protect the data using a security solution that delivers data-centric, file-level encryption that is portable across all computing platforms and operating systems and works within a private, public or hybrid cloud computing environment.

Now a day's preventing security threats coming from outside cloud is not a big deal. if it is within the organization ? Hence it is recommend creating usage policy statements that outline users' roles and responsibilities with regard to security. Create a general policy that covers all network systems in cloud and data within the company. If any company has identified specific actions that could result in punitive or disciplinary actions against an employee, these actions and how to avoid them should be clearly articulated in this document.

Low Risk Systemsor data or virtual machines in cloud that if compromised (data viewed by unauthorized personnel, data corrupted, or data lost) would not disrupt the business or cause legal or financial ramifications. The targeted system or data can be easily restored and does not permit further access of other systems.

Medium Risk Systemsor data or virtual machines in cloud that if compromised (data viewed by unauthorized personnel, data corrupted, or data lost) would cause a moderate disruption in the business, minor legal or financial ramifications, or provide further access to other systems. The targeted system or data requires a moderate effort to restore or the restoration process is disruptive to the system.

High Risk Systems or data or virtual machines in cloud that if compromised (data viewed by unauthorized personnel, data corrupted, or data lost) would cause an extreme disruption in the business, cause major legal or financial ramifications, or threaten the health and safety of a person. The targeted system or data requires significant effort to restore or the restoration process is disruptive to the business or other systems.

Next assign this risk level to each core network devices, distribution network devices, access network devices, network monitoring devices in cloud. If we implement the same thing at Network equipment such as switches, routers, DNS servers, and DHCP servers can allow further access into the network, and are therefore either medium or high risk devices. It is also possible that corruption of this equipment could cause the network itself to collapse. If we do so 80% problem is slaved. Once you've assigned a risk level, it's necessary to identify the types of users of that cloud environment.

Admin of that cloud: responsible for internal users and network resources.

Internal users: It helps to provide limitation for local users while accessing cloud services.

Outside Partners External users with a need to access some resources.

VII. CONCLUSION

A cloud is an attractive infrastructure solution for web applications since it enables web applications to dynamically adjust its infrastructure capacity on demand. Hence along with services is important to concentrate on security also. Policy management may solve security problem. But it will not give 100% alternate for the security problems in cloud services. Hence we have to check alternates for every time. Because security problems in cloud computing does not have the permanent solutions.

REFERENCE

[1].SecurityasaServicehttps://cloudsecurityalliance.org/research/secaas/

[2].Riskmanagementhttp://www.whatisriskmanagement.net/

[3].webdatabases
http://www.systemdisc.com/what-are-web-databases

[4].Emailintelligencehttp://en.wikipedia.org/wiki/2012_Stratfor_email_leak

[5]. Email encryption
http://en.wikipedia.org/wiki/Email_encryption

AUTHORS PROFILE

Tejaswi.K has received B.Tech degree in Computer Science and Engineering branch. She is now pursuing M.Tech (Computer Science and Engineering) from Anurag Group of institutions (Formerly CVSR College of Engineering).

Mrs.Sridevi.M has received B.Tech and M.Tech degrees in Computer Science and Engineering branch. She is working as an Associate Professor, Department of Computer Science and Engineering in Anurag Group of institutions (Formerly CVSR College of Engineering).She has 8 years of teaching experience.

Mr. Vishnu Murthy G received his B.E and M.Tech degrees in Computer Science and Engineering. He is having 15 years of teaching experience. He is presently pursuing his Ph.D. in JNTU, Hyderabad and is the Head of the Computer Science and Engineering Department, Anurag Group of institutions (Formerly CVSR College of Engineering). He has organized and attended various workshops and conferences at National and International level. He has been the resource person for Institute of Electronic Governance and BITS off campus programs. He is the Life Member of ISTE, IEEE, ACM, CRSI & CSI. He had 5 publications in international journals and presented 2 papers in conferences. His areas of interest include Software Engineering, Information Security and Image Processing.