Database security in a cloud computing environment

By **Tai Cleveland**, CTU student | Security, Database Security

November 13, 2009, 8:52 AM — Abstract

The use of the cloud computing environment to cater to the demands of users in the internet has made database security a critical issue. Security is a critical issue in cloud computing due to the variety of IT services that can be provided through a cloud environment. This paper highlights that database security should ensure data confidentiality, integrity and availability on any system. Included in the discussion are the latest security methods and current trends to protect the system against potential threats. Cryptography, secret key methods, digital signatures and certificates are introduced as means to protect databases.

The paper cites the work of authorities on the three fundamental approaches to monitoring database activity. IT professionals are encouraged to acquaint himself also of the limitations of database monitoring. The Mandatory Access Control (MAC), Lattice-Based Access Control (LBAC), and Role-Based Access Control (RBAC) are considerations in the planning and implementation of access control mechanisms. In addressing securities, one needs to tackle network security, physical security, data security, and applications and host security. This paper offers insight to security challenges, discusses techniques and methods used in securing a database as well as security features and products, and the different types of security measures.

Discussion

In moving a database to a cloud computing environment, there is a need to identify security requirements. In a cloud computing environment where dynamically scalable and virtualized resources are available for use over the Internet (Gartner, 2008), database security is a challenge due to virtual set up and use. Security is critical due to the varied IT services that can be provided through a cloud. Said Gartner:

The types of IT services that can be provided through a cloud are wide-reaching. Compute facilities provide computational services so that users can use central processing unit (CPU) cycles without buying computers. Storage services provide a way to store data and documents without having to continually grow farms of storage networks and servers. SaaS companies offer CRM services through their multitenant shared facilities so clients can manage their customers without buying software. These represent only the beginning of options for delivering all kinds of complex capabilities to both businesses and individuals (Gartner, 2008).

Consumer and corporate trust in public or private institutions often depend on the security of the information held in their databases. Database security assures data confidentiality, integrity, access, and availability on any system, which is based on a comprehensive security policy.

It is important to recognize the latest security methods and current trends to block the system against potential threats. Existing methods and approaches are then applied to the current cloud technology setting. In this paper, we first survey the database security techniques and approaches used and summarize some of the known techniques and approaches as well as security models. A

discussion on private cloud databases versus public cloud databases will offer insight to security challenges. A detailed analysis of database security challenges on a cloud computing environment offers information on how to validate, quantify and manage security services.

There are techniques and approaches currently used for database security. Monitoring, electronic signatures, vulnerability assessment, data masking, encryption, are all currently available to protect data when transmitted across sites and enforcing access control based on policies set for database inquiries.

Hackers attack databases to gain access to personal data, perhaps to use it for personal gain or for some illegal practice. A company can adopt database monitoring as one of its security controls. Concern over the protection of database from hacker attacks may have been reinforced by the report of Privacy Rights Clearinghouse, a web site devoted to maintaining a record of all data security breaches in the US. Nair cited the report in her article:

The Privacy Rights Clearinghouse reported that laptops are the number one source of data breach incidents (47 percent), databases are next (40 percent), then tapes (11 percent) and e-mail (2 percent). Looking at the same data based on the amount of data lost, databases are the number one source (64 percent), laptops are next (25 percent), then tapes (10 percent) and finally e-mail (1 percent) (Privacy Rights Clearinghouse, as cited in Nair, 2008, 1).

Nair provided an overview on the three fundamental approaches to address the issue of monitoring database activity. In the overview, Nair described the three approaches:
A software-only approach typically requires turning on some level of native database auditing from which the software agent gathers data. (…) A relatively new approach to database monitoring is to use a network appliance to monitor database traffic. These appliances either run as passive devices connected to a mirroring or Switched Port Analyzer (SPAN) on a switch, or act as in-line devices, i.e., essentially database firewalls. (…) A combination of network appliance and local software auditing is an ideal way to address data activity monitoring in an enterprise. This maximizes the overall coverage of the auditing solution (Nair, 2008, 2-3).

While database monitoring may protect a company's database, the IT professional should also evaluate the shortcomings of this method as it applies to the organization. He should particularly pay attention to such limitations as stored procedures and triggers, encrypted network traffic, connection-pooled environments and Support for MSM or security incident and event management (SIEM) systems (Nair, 2008, 3).

Sometimes IT practitioners miss the opportunity to provide adequate protection for the organization's database. This is of particular concern since hackers are out to access information that has monetary value. Database security assessment includes regularly auditing the database servers to help security staff identify configuration issues and policy and compliance violations (Rapid 7). An organization's database may be designed differently from other databases in order to meet business requirements. Databases can be protected through period assessment to prevent malicious attacks. The first step to take is to set up an inventory of databases in the organization. Assessment takes the form of evaluating the database in relation to the identified threats. The results of the assessment can be used to strengthen the database.

Cryptography is one of the methods used in securing a database in a cloud computing environment. It presents a range of methods for taking comprehensible, readable data, and converting it into unreadable data for the point of secure transmission, and then using a key to

change it back into readable data when it reaches its destination (Nicholas Galbreath & Nick Galbreath, 2002). The goal of cryptography reaches beyond on not only making data unreadable, it also extends into user authentication which provides the user with guarantees that the encrypted message originated from a reliable source.

Some methods of cryptography use a secret key to allow the user to decrypt the message. Secret key ciphers carry out encryption and decryption using the same key, and cryptographic hashes must be computed and confirmed using the same key (Nicholas Galbreath & Nick Galbreath, 2002). Basically, a cipher is a function that locates a message, identified as plaintext, into an unreadable form, branded as ciphertext, by use of a key. This is known as encryption. A user cannot do the inverse transformation, the decryption, or turning the cipher text back into its original plaintext form without a key. To be effective, a cipher must be protected and must be functional. Most users opt for longer keys since it is more secure. But keys of more than a few bytes are easily forgettable. Cryptographic hashes protect against malicious modification of a message.

A hash or message digest is a function that takes an arbitrary-sized message and returns a number based on the message's contents. Hash functions are sometimes used in combination with private key or public key cryptography. This is a type of one-way encryption, which applies an algorithm to a message, such that the message itself cannot be recovered (Nicholas Galbreath & Nick Galbreath, 2002). Unlike key-based cryptography, the goal of the hash function is not to encrypt data for later decryption, but to generate a somewhat digital fingerprint of a message. The value resulting from applying the hash function can be re-calculated at the receiving end, to make certain that the message has not been tampered with during transmission. Then, key-based cryptography is applied to decode the message.

One of the common secret key methods is to use a password or passphrase that is used to create a key. The most common secret key cryptosystem is the Data Encryption Standard (DES), or the more secure Triple-DES which encrypts the data three times. An evident technique is to hash the password bytes in order to generate new bytes to use a key. While this works, the problem is that the amount of possible passwords is much smaller than the possible number of keys. If the password is nine characters made from the set of upper- and lowercase letters, numbers, and symbols for a total of 72 symbols, it means a user only have a 55-bit key (Nicholas Galbreath & Nick Galbreath, 2002). Instead of trying to strengthen the key, a database attacker would find it easier to try every password instead in a cloud computing system. A user can solve this problem by making the password longer.

Also common are systems that make use of a public key cryptography system, such as the Diffie-Hellman key agreement protocol. This system uses two keys that work together. First is a public one, which anyone can access, and second, is a private one, which is kept confidential by the party receiving the data. When a user wants to transmit a secure message to someone, all a user has to do is encrypt that message using the recipient's public key. But once encrypted, the recipient must use his or her private key to decrypt it (Martin E. Hellman, 2002).

Digital signatures and certificates are also techniques to protect data. Electronic signatures can be defined as any electronic process signifying an approval to terms, and/or a document, presented in electronic format (Security Matters).

A digital certificate is an electronic attachment applied to a program, database, or other electronic document (Patricia Cardoza, Teresa Hennig, Graham Seach & Armen Stein, 2004). The digital

certificate classifies the person or entity that published it and the date and times that it was published. The certificate can also spot the reason of the certificate and the purpose of the program, database, or electronic document to which it applies. Therefore, a digital signature is a means to "apply a digital certificate to programs, databases, or other electronic documents so that a user of that program, database, or document can confirm that the document came from the signer and that it has not been altered since it was signed" (Cardoza, Hennig, Seach & Stein, 2004). If the program, database, or document is changed after it has been digitally signed, the signature is immediately removed. This aspect means that a user is ensured that nobody can launch viruses after the signature is applied. A user will have to acquire a digital certificate in order to give his or her database a digital signature.

There are actually two types of digital certificates. They are commercial and internal digital certificates. Commercial certificates are attained through a commercial certification authority such as Verisign, Inc. (Cardoza, Hennig, Seach & Stein, 2004). Internal certificates are deliberately for use on a single computer or within a single organization and can be accessed from an organization's security administrator or produced using the Selfcert.exe program (Cardoza, Hennig, Seach & Stein, 2004). The Selfcert.exe program is a stand-alone program for creating one's own digital certificates.

To snag a commercial certificate, a user must request and buy one from an authorized commercial certificate authority vendor. When the vendor sends one of these certificates, the recipient will receive instructions about how to set up the certificate on the computer and how to use it with a Microsoft Access application. The certificate a user will need for Access databases is called a coding signing certificate. Also, there are certificates that are suitable for "Microsoft Authenticode" technology (Cardoza, Hennig, Seach & Stein, 2004). The commercial certificate offers full protection of one's database for legitimacy. Since the digital certificate is removed if the file is modified, a user can guarantee that the database will not be authenticated if anyone tinkers with it. Likewise, commercial certificates present protection for users. If someone obtains a certificate and then uses that certificate for malicious purposes, the commercial authority will cancel the certificate. Then, anyone who uses software that is signed with that certificate will be informed of its cancellation.

Internal certificates are intended for use on a single computer or within a single organization. An internal certificate offers the same protection as the commercial certificate. Internal certificates can be formed and handled by a certificate authority within an organization with the use of a Microsoft Certificate Server tool. A user can make a certificate for his or her own computer by using the Selfcert.exe (Cardoza, Hennig, Seach & Stein, 2004).

All of these security methods are used for securing the database within the computer. But there is a major difference between computer security and database security. Computer security has expanded to signify issues with regard to the networked use of computers and their resources (Jane F. Kinkus, 2002). A computer security model is a design for indicating and implementing security policies. Database systems deals with many different types of objects and the access controls are the important elements in designing security models for database security.

The objectives of confidentiality, integrity and availability comprise key components of computer security. The three objectives can be illustrated by the following examples: This objectives appear in practically every information system. In a payroll system, for example, confidentiality is concerned with preventing an employee from finding out the boss's salary; integrity, with preventing an employee from changing his or her own salary; and availability, with

ensuring that paychecks are printed on time. Similarly, in a military command and control complex, confidentiality is concerned with preventing the enemy from determining the target coordinates of a missile; integrity, with preventing the enemy from altering the target coordinates; and availability, with ensuring that the missile is launched when the order is given (Sandhu, 1993).

While confidentiality, integrity, and availability are the chief concerns of a computer security administrator, privacy is perhaps the most important aspect of computer security for Internet users (Kinkus, 2002). Privacy on the Internet is about shielding one's personal information, even if users may feel that they have nothing to conceal when they are signing up with a website or Internet service. Kinkus explained why:

(…) privacy on the Internet is about protecting one's personal information, even if the information does not seem sensitive. Because of the ease with which information in electronic format can be shared among companies, and because small pieces of related information from different sources can be easily linked together to form a composite of, for example, a person's information seeking habits, it is now very important that individuals are able to maintain control over what information is collected about them, how it is used, who may use it, and what purpose it is used for (Kinkus, 2002).

Controlling access to information systems and associated networks is required for the preservation of its confidentiality, integrity, and availability. Confidentiality promises that the information is not revealed to unauthorized persons or processes. Integrity makes certain that the internal data is consistent with the prevention of altering information by unauthorized users. And availability reassures that a system’s authorized users have judicious and continual access to the information in the system. The additional access control objectives are reliability and utility (Ronald L. Krutz & Russell Dean Vine, 2002).

There are three things to consider for the planning and implementation of access control mechanisms that are the threats to the system, the system’s vulnerability to these threats, and the risk that the threat might pose. Access controls are applied to alleviate risk and trim down the potential for loss. Access control models are split into three categories or models. They are Mandatory Access Control (MAC), Lattice-Based Access Control (LBAC), and Role-Based Access Control (RBAC).

Mandatory Access Control is an access policy determined by the system, not the owner. MAC is used in most multilevel systems that process extremely sensitive data, such as confidential government and military information. A multilevel system is a sole computer system that manages multiple classification levels between subjects and objects (Krutz & Vines, 2002).

Lattice-Based Access Control, known as a label-based access control restriction, is used for complex access control decisions concerning multiple objects and subjects. A lattice model is a partial order set that describes the utmost lower-bound and least upper-bound values for a pair of elements, such as a subject and an object (Krutz & Vines, 2002). A lattice is used to characterize the levels of security that an object may have and that a subject may have access to. The subject is only permitted to access an object if the security level of the subject is greater than or equal to that of the object. A number of models has been developed to provide theoretical and conceptual foundations in relation to computer security (Sandhu, 1993).

And lastly, Role-Based Access Control, sometimes referred to as role based security, is a method of restricting system access to authorized users (David Ferraiolo & D. Richard Kuhn, 1992). Sandhu explained the notion of RBAC:

The central notion of RBAC is that permissions are associated with roles, and users are assigned to appropriate roles. This greatly simpli_es management of permissions. Roles are created for the various job functions in an organization and users are assigned roles based on their responsibilities and quali_cations. Users can be easily reassigned from one role to another. Roles can be granted new permissions as new applications and systems are incorporated, and permissions can be revoked from roles as needed (Sandhu, 1995).

RBAC is used in commercial applications and also in military systems, where multi-level security requisites are also in existence. RBAC directs collections of permissions that may incorporate complex operations such as an e-commerce transaction, or may be as simple as read or write. In RBAC, access is controlled at the system level outside of the user's control since users are not assigned permissions directly, but only obtain them through their role (or roles). Management of individual user rights becomes a matter of merely conveying suitable roles to the user, thus simplifying common operations, such as adding a user, or changing a user's department (Ferraiolo & Kuhn, 2002). A role in RBAC can be also cited as a set of permissions.

Controls can be preventive, detective, or corrective (Krutz, & Vines, 2002). Preventive controls are fitted in place to restrain damaging occurrences, detective controls are established to determine detrimental occurrences, and corrective controls are used to reinstate systems that are victims of harmful attacks.

To employ these measures, controls can be administrative, logical or technical, and physical. Administrative controls contain procedures and policies, background and work habit checks, security training, review of vacation history, and better supervision. Logical or technical controls engage the restriction of access to systems and the protection of information. Instances of these types of controls are encryption, smart cards, access control lists, and transmission protocols (Krutz & Vines, 2002). Generally, physical controls integrate sentinels and building security such as the fastening of doors locks, the securing of servers, desktops, or laptops, the protection of cables and wiring, the partition of duties, and the backing up of both sensitive and non-sensitive files.
Controls give liability for individuals who are obtaining sensitive information. This accountability is established through access control mechanisms that necessitate identification, authentication, and overall security.

In establishing general security, it requires detailed planning and policy. An assessment of an organization’s exposure and risks are part of the planning process. To protect the data from internal and external threats, database security evaluation is required when there is a system update or any changes applied to the database setup.

Securing a database goes beyond encrypted data and passwords. A database administrator should also be aware of the vulnerabilities by keeping confidential data secure from internal or external database prowlers even if the password has been compromised. The database security area faces several new challenges. Factors such as the advancement of security concerns, the blocking of access to critical data, new computing paradigms and applications, such as cloud computing and on-demand business, have initiated both new security requirements and new contexts in which to apply and probably widen existing security approaches.

While database security is mostly important, it is also necessary to acquire Internet protection. Internet security involves the protection of a computer's internet account and files from intrusion of an unauthorized user. Basic security measures involve protection by well-chosen passwords, change of file permissions, and back up of computer files and data (Man Young Rhee, 2003). Security will probably always be high on the IT agenda just because cyber criminals know that a winning attack is very advantageous.

Internet users should always be aware and vigilant especially when dishing out personal information. Even if a computer isn't used for anything serious, users must need to run security software such as an antivirus and a firewall. These programs will keep the computer protected from viruses and other malware that can multiply through email or other methods. In email, there are email encryption protocols to authenticate email messages.

To move a database in the cloud, there is going to be inactivity when accessing it from a user's location. Microsoft recommends running applications that are using the database in the cloud on the Azure Platform, so the latency is minimal. When one positions an application on Windows Azure and provision an SDS server, the two are going to be co-located, to provide low latency between the data and the application (Alin Irimie, 2009).

Like with any other database, corruption of data can transpire in the cloud database as well. Microsoft has mechanisms in place to pull through from data corruption mostly by keeping database copies on multiple servers; however, they do not offer any backup of the database. In some of the PDC 2008 presentations, there will be a database backup/restore and geo-replication such as synchronous (simulated set spans datacenters) and asynchronous (self-determining duplication sets in different datacenters) (Irimie, 2009).

The types of databases that are applied in a cloud computing environment are operational databases, end-user databases, external databases, hypermedia databases, and navigational databases. Operational databases include customer, personal, and inventory databases. End-user databases comprise of a range of data files developed by end-users. Collection of documents in spreadsheets, word processing and even downloaded files are examples of end-user databases. Access to a score of information from an external database is accessible for a fee from commercial online services with or without charge from many sources in the Internet. Hypermedia databases are a set of interconnected multimedia pages at a web site. It features a homepage and other hyperlinked pages of multimedia or mixed media like text, graphic, images, audio, and video. Lastly, navigational databases have objects that are found principally by following references from other objects.

Databases also differ when it comes to private or public databases in a cloud computing environment. A private cloud database is when an organization possesses its own database applications, its servers, and no other entity outside of the organization is allowed to have an access. The servers are dedicated servers to be used by the organization only. Private databases are also an assemblage of names from external sources that are used for a particular user's exclusive prospecting purposes. A public cloud database is used by any entity worldwide and no single outside entity takes ownership of the database except the cloud service provider. The data from the database could be private or public data depend on types of data and organization that owns the data.

Speaking of public databases, such databases that are moved in a cloud computing environment are open to the public so securing its sensitive data is already a challenge. Any IT outsourcing that

involves network infrastructure, security monitoring, remote hosting, are all forms of cloud computing (Bruce Schneier, 2009) so critical data can be found on some cloud computer with some user's spreadsheets floating in Google's servers. According to Bruce Schneier's blog about cloud computing security, it all boils down to trust actually. There should be a grain of trust in the CPU manufacturer, the purchased hardware and operating systems, the software vendors, the Internet Service Provider (ISP), and even the customers. Any one of these can dent database security by crashing the systems, damaging the data, and allowing an intruder to get access to the systems. There really is no choice but to "blindly trust the security of the IT providers we use" (Schneier, 2009).

In addressing securities, one needs to tackle network security, physical security, data security, and applications and host security too. Network security includes provisions made in a principal computer network infrastructure, policies implemented by the network administrator to protect the network and the easily-reached resources from an unknown access, and constant supervision and measurement of its usefulness (William Stallings, 2007). Network security starts from authenticating any user, typically with a username and a password. Honeypots, used basically to decoy resources, could be installed in a network as surveillance tool. For basic network protection, a strong firewall and proxy should be set up to keep unauthorized persons out.

Physical security defines both measures that thwarts or dissuades attackers from accessing a facility, information, or resource stored on physical media. It can be as simple as a bolted door or as complex as having security guards around. Physical security exists in order to prevent unauthorized persons from breaking in a physical facility (Lawrence J. Fennelly, 2004). The technology used for physical security has changed over the years. Examples of physical security include video monitoring to verify malicious movement, electronic access control to administer the control and handling of mechanical keys to locks or property within a building, and intrusion detection alarm systems to capture a response.

Data security is an approach of making certain that a data is kept out of harm's way from exploitation and that access to it is duly controlled. It also helps in protecting personal data (David Salomon, 2003). There are different data security technologies such as disk encryption, back ups, data masking, and data erasure. Disk encryption is about encryption technology that encrypts data on a hard disk drive. It usually takes form in either software or hardware. File back ups are used to warrant that lost data can be recovered. Data masking is the process of masking particular data within a database table or cell to assure that data security is sustained and critical customer information is not disclosed outside of an authorized environment. And, data erasure is a software-based overwriting technique which completely destroys all electronic data stored on a hard drive or other digital media to certify that no sensitive data is leaked out.

Applications security covers measures taken to prevent omissions in the security policy of an application or the causal system through defects in the design, consumption, or maintenance of the application. Applications only handle the use of resources given to them. Consecutively, they verify the use of these resources by users of the application through application security. On the other hand, host security policies include maintaining strong security on host especially since if the external security fails, the network is wide open for an attack. Host security may depend on vendor-provided security features but generally, login passwords are required for a user to gain access to the system.

Scalability of security on a cloud environment allows consumers of cloud computing resources to rise up promptly to manage prickles in computing loads, or visibly distribute computation across

partner cloud service providers. However, this distribution of data and the different sensitivities of this data have a negative aspect as it may run badly of risk, or compliance concerns, and cause risks to end-users and to businesses that supply cloud services (Seth Hanford, 2009). Data that dwells in the cloud and has been distributed to several servers worldwide may have been simulated to systems in other countries with hugely different policies.

Network security mechanisms in a cloud address impending risk management and application distribution issues. Creating a cloud computing infrastructure will move sensitive data out of the enterprise environment and in to the cloud, meaning professionals need to improve security and revise their architectures. If the network is not appropriately architected and managed, security risks will abound. Enterprises should note how to secure network mechanisms such as modems, crypto-capable routers, and dial-back systems. It's also essential to build systems and networks in such a way that the user is not frequently reminded of the security system.

There is also available security features for emerging cloud applications. A cloud application controls the cloud in software architecture, often removing the need to install and run the application on the user's own computer, thus lessening the burden of software maintenance and operation. Cloud applications include peer-to-peer or volunteer computing (Skype, Bittorrent), web application (social networking sites), Software-as-a-Service (or SaaS, which include Google Apps), and software plus services (Microsoft Online Services). Password encryptions and firewalls are necessary precautions in sending out information in these cloud applications. However, companies must carefully regard the implications of immensely scalable design, storage, and computing. This is especially true if those services are outsourced to cloud providers and not directly under company control.

A leaked data is a nuisance especially if that data is a critical one. There are various access control mechanisms available such as firewalls, encryption, and evidently defined permissions and access control lists. Yet sometimes, these defenses aren't functioning effectively. Protection techniques are valuable for preventing data leaks through employee indolence, unintentional or lackadaisical policy violation, or just plain brainless user actions. But they are not going to deter a motivated and malicious attempt at data theft. If security is about layered protections (security guards for that matter) and trying to stay one step ahead of at least most of the bad and the careless, these products have a lot of security guarantees.

There is no shortage when it comes to the current security products for databases on a cloud computing environment. Some of these products are DbEncrypt, Enzo, and Secure.Server (Timberline Technologies, 2005). DbEncrypt is a database encryption solution that contains an entire list of encryption algorithms to choose from, templates, and a discerning point-and-click management interface. Enzo presents a four-dimentional database access control solution that permits administrators to identify unprecedented granular database access rules. And Secure.Server checks user authorization according to identity, position, or organization before granting access rights.

In terms of database security, it looks like stealing websites and FTP credentials are the latest rage cracking websites and spreading malware. Only recently, attackers have targeted legitimate websites. Websense, Inc. (a security vendor) researchers claim that the attackers are simply instilling malicious JavaScript code into sites by logging in with stolen usernames and passwords (Rob Westervelt, 2009). So users should always change passwords from time to time and not leave any confidential information such as usernames and passwords out in the open.

Suppliers of database security services such as Websense, Inc. have been providing equipment from web, data, to email security products. According to its website, “Websense software and hosted security solutions help organizations block malicious code, prevent the loss of confidential information and enforce Internet use and security policies” (Websense, Inc.). The company’s most widely known product is the ThreatSeeker Network which provides users the most advanced protection possible from unwanted content and malicious threats.

These products are reasonably priced as well and provide us the ability to detect and respond to potential threats and attacks. Once a company measures in what it would cost to manage its own data center with the approximates of the online feature’s implementation, the company will realize that the investment will be worth it for a long term which is actually based on cost histories of cloud providers as well as the company’s own calculations (John Allspaw, 2008). The cloud approach to systematize business is secure and proficient. Cloud computing provides a convincing opening to reach a more efficient solution, and bring cost savings together with scalability and extensibility.

This paper offers insight to security challenges, discusses techniques and methods used in securing a database as well as security features and products, and the different types of security measures. Cloud computing has developed from being a capable business concept to one of the fastest rising segments in the information technology industry. Businesses gradually understand that by tapping into the cloud environment, they can achieve fast access to the best business applications or considerably improve their infrastructure resources, all at tiny fraction of a cost. But as more databases are placed in the cloud, concerns are beginning to rise about just how safe and secure an environment it is. We recognize that the transition to a cloud computing paradigm presents a number of challenges.

Issues associated with information security, dependability, and service level compliances challenge critical systems. Furthermore, we have identified what we consider the key points on how to secure a database in a cloud computing environment. Greater analysis and re-engineering are essential to attain the full benefits of a cloud computing environment. Organizations must consider the remaining complexities when moving to the cloud and careful planning is necessary.

REFERENCES

1. Allspaw, John. (2008). The Art of Capacity Planning. O'Reilly. Retrieved July 6, 2009, from: http://books.google.com.ph/books?id=Yi3trjJ1JuQC&pg=RA1PA108&dq=cloud+computing&hl=en

2. Alphabetical List of Database Security Products. Timberline Technologies. Retrieved July 9, 2009, from: http://www.timberlinetechnologies.com/products/database.html

3. Cardoza, Patricia, Hennig, Teresa, Seach, Graham & Stein, Armen. (2004). Access 2003 VBA Programmer's Reference. John Wiley and Sons. Retrieved July 9, 2009, from: http://books.google.com.ph/books?id=NafXqquUxbsC&pg=PA634&dq=Digital+Signatures+and+Certificates&hl=en

4. Fennelly, Lawrence J. (2004). Effective Physical Security. Butterworth-Heinemann. Retrieved July 10, 2009, from: http://books.google.com.ph/books?id=T2Vd9D3iRw8C&printsec=frontcover&dq=physical+security&hl=en

5. Ferraiolo, David F. & Kuhn, D.Richard (1992, October). "Role Based Access Control". 15th National Computer Security Conference. Retrieved July 10, 2009, from: http://csrc.nist.gov/groups/SNS/rbac/documents/ferraiolo-kuhn-92.pdf

6. Galbreath, Nicholas & Galbreath, Nick. (2002). Cryptography for Internet and Database Applications. John Wiley and Sons Retrieved July 8, 2009, from: http://books.google.com.ph/books?id=YW6GJCj1Rf8C&pg=RA3PA267&dq=database+security&lr=&hl=en

7. "Gartner Says Cloud Computing Will Be As Influential As E-business". (2008, June 26). Gartner. Retrieved July 6, 2009, from: http://www.gartner.com/it/page.jsp?id=707508

8. Hellman, Martin E. (2002). An Overview of Public Key Cryptography. IEEE Communications Magazine. Retrieved July 8, 2009, from: http://www.comsoc.org/livepubs/ci1/public/anniv/pdfs/hellman.pdf

9. "Improving Web Application Security: Threats and Countermeasures." Microsoft Corporation. Retrieved July 9, 2009, from: http://msdn.microsoft.com/en-us/library/ms994920.aspx

10. Irimie, Alin. (2009 May 27). SQL Data Services. Your Database in the Cloud. Retrieved on July 8, 2009, from: http://www.azurejournal.com/2009/05/sql-data-services-your-database-in-the-cloud/

11. Kinkus, Jane F. (2002). Computer Security. Issues in Science and Technology Librarianship. Retrieved July 9, 2009, from: http://www.istl.org/02-fall/internet.html

12. Krutz, Ronald L. & Vines, Russell Dean. (2002). The CISSP Prep Guide: Gold Edition. John Wiley and Sons. Retrieved July 9, 2009, from: http://books.google.com.ph/books?id=kB1Vbpz_5sgC&pg=PP1&dq=Ronald+L.+Krutz+%26+Russell+Dean+Vine&hl=en

13. Nair, Sushila. (2008). The Art of Database Monitoring. ISACA Journal (3). Retrieved September 15, 2009, from: http://www.itgi.org/AMTemplate.cfm?Section=2008&Template=/ContentManagement/ContentDisplay.cfm&ContentID=49695

14. Rapid 7. Database Vulnerability Assessment. Retrieved on September 15, 2009, from: http://www.rapid7.com/soln/database-java.jsp

15. Rhee, Man Young. (2003). Internet Security. John Wiley and Sons.
Retrieved July 8, 2009, from
http://books.google.com.ph/books?id=bJJUVNGbrLsC&printsec=frontcover&dq=internet+security&lr=&hl=en

16. Salomon, David. (2003). Data Privacy and Security. Springer.
Retrieved July 10, 2009, from:
http://books.google.com.ph/books?d=z3foyEooUC&printsec=frontcover&dq=data+security&lr=&hl=en.

17. Sandhu, Ravi, S. (1993). Lattice-Based Access Control Models. Retrieved on September 15, 2009, from:
http://profsandhu.com/journals/computer/i93lbacm(org).pdf

18. Security Matters. Retrieved on September 15, 2009, from:
http://blogs.adobe.com/security/2008/02/so_what_is_an_electronic_signa.html

19. Schneier, Bruce. (2009, June 4). Cloud Computing. Schneier Blog.
Retrieved July 8, 2009, from:
http://www.schneier.com/blog/archives/2009/06/cloud_computing.html

20. Westervelt, Rob. (2009, June 04). Stolen FTP Credentials Likely in Massive Web Attack.
Threatpost. Retrieved July 9, 2009, from:
http://www.threatpost.com/blogs/stolen-ftp-credentials-likely-massive-web-attacks