ABSTRACT
Cloud computing is changing businesses and governments. It offers flexible computation resources in a model where customers only pay for resources they use. This leads to cost savings when compared to a situation where organizations manage their own server farms. Very often such servers are running at a very low utilization level, which is partly because of old habits that lead to not placing more than one server on a single physical server.

The benefits of cloud computing are many, but it also introduces new issues regarding security. Often customers feel like they are giving up the control over their data when they make the move to cloud. For the same reason many organizations are yet to make the move.

This paper is a survey to some of the most recognized and feared issues in cloud security and also aims to bring forward current solutions for those security issues, or ways to mitigate the risks of making the move to the cloud.

Categories and Subject Descriptors
D.4.6 [Security and Protection]

General Terms
Design, Security

Keywords
Cloud Computing, Cloud Security

1. INTRODUCTION
Cloud computing has caused a shift in technology. This shift has changed the way businesses, governments and other actors deploy and deliver IT services. Cloud computing provides customers services varying from infrastructure and network to applications in the cloud. By making the move to the cloud, cloud consumers no longer have to make investments on new infrastructure, software licenses or personnel for maintaining that infrastructure and those applications.

The flexibility or elasticity of the cloud platform removes the need for organizations to invest in infrastructure capacity that is only used during certain peak periods, e.g. during holiday seasons.

However, as organizations are planning on making the move to the cloud, they need to consider a wide range of security issues introduced by the way cloud computing works. Cloud computing services are usually accessed over the internet, and the internet is known be host to a wide range of threats, such as malware, viruses, and criminal organizations targeting their victims with attacks towards web services and infrastructure. Also, as cloud computing platforms are usually shared among several customers, this multi-tenancy (multiple customers sharing applications and/or computer resources) introduces threats specific to shared platforms. One must secure himself or herself from cross-VM attacks and malicious virtual machine images.

As customers data moves from inside the organization to the cloud, the customer often loses most of the control over that data. And without transparency from the cloud service provider there is little ways to verify that the integrity if one’s data is intact and that the data itself is available to the customer now and in the future.

Organizations that need to comply to regulations, such as HIPAA or PCI DSS, imposed on them need to work with the cloud service provider in order to agree on the responsibilities each party has in securing the applications and infrastructure as required in the regulations.

The rest of the paper is organized as follows. In the next section the definition of cloud computing and its deployment and service models will be introduced. In section 3 some of the top cloud security threats will be introduced and section 4 will introduce known solutions or mitigation methods regarding those issues. Section 5 will conclude this paper.

2. CLOUD COMPUTING
Cloud computing enables on-demand access to a shared pool of resources. These resources can be rapidly provisioned to match customer needs and the process of provisioning more resources usually does not require a customer to directly interact with the cloud service provider.

Aspects of cloud computing such as elasticity, pay-as-you-go payment model, and the lack of need to invest money and time to set up a data center are, among other things, reasons that drive customers to make the move to the cloud.
2.1 Definition
Only a few years ago researches were struggling with how to define cloud computing. [4] lists over 20 different definitions of cloud computing in 2008.

Nowadays, the definition by National Institute of Standards and Technology (NIST) [13] is widely accepted as the standard definition of cloud computing. It lists five essential characteristics that make the cloud. These characteristics are:
- **On-demand self-service**, meaning that the cloud user can provision resources automatically without the need of human interaction with the cloud service provider.
- **Broad network access**, meaning that customers can access their cloud resources over the network without the requirement of a homogenous set of client platforms.
- **Resource pooling**, meaning that the cloud service provider maintains pools of resources. These pools are used to satisfy the needs of multiple customers using a multi-tenant model.
- **Rapid elasticity**, meaning that resources can be provisioned and released in an elastic manner. This enables the customer to react to changes in demand either manually or automatically.
- **Measured service**, meaning that the customer only pays for the resources he or she uses. This pay-as-you-go model requires that the cloud service providers support such metering capabilities.

Combined, these characteristics differentiate cloud computing from grid computing. The two share similar visions, and therefore there has been confusion on the matter of separating clouds from grids [4].

2.2 Service Models
Cloud service models are best used to describe the division of responsibilities between the customer and the cloud service provider. For example, IaaS customers have responsibility over the guest operating systems and software running on top of that operating system, whereas SaaS customers are rarely responsible for anything besides a few configuration parameters of the service.

2.2.1 **Infrastructure-as-a-Service (IaaS)**
IaaS customers have the capability to provision processing power, storage, networks, and other resources. However, the customer does not control the infrastructure, but does have control over the deployed guest operating systems and applications. A limited access to networking component configurations (such as host firewalls) may be possible.

2.2.2 **Platform-as-a-Service (PaaS)**
PaaS offerings enable customers to deploy their own custom-made software onto the cloud. The software must be developed using the programming languages, service stacks, libraries and tools supported by the cloud service provider.

2.2.3 **Software-as-a-Service (SaaS)**
SaaS offerings enable to customer to use applications deployed on a cloud infrastructure by the cloud service provider. These applications are usually reachable through thin and thick clients. The customer is only responsible for any customer-specific configurations made to the application.

2.3 Deployment Models
NIST categorizes four different cloud deployment models [13]. The differences lie in the responsibility of the management of the cloud architecture and in the tenancy of the cloud.

2.3.1 **Private Cloud**
Private clouds are deployed for the use of a single organization. The organization may own and/or manage the cloud, or it may be partially or completely managed by a third party. An organization’s private cloud may exist on or off premises.

2.3.2 **Public Cloud**
A public cloud is the opposite of a private cloud. A public cloud is deployed for open use of the public. The cloud exists on the premises of the cloud service provider, and the service provider can be a business, academic, or government organization or a combination of them.

2.3.3 **Hybrid Cloud**
A hybrid cloud is a combination of any of the three cloud deployment models, but these two or more unique entity clouds are interconnected in a way that enables data and application portability between the two.

2.3.4 **Community Cloud**
A community cloud is shared between two or more individual actors who have joint concerns or goals, such as common compliance requirements, policies or missions. A community cloud may be managed by one or more of the community members or by a third party. The cloud may exist on or off the premises of the community members.

3. CLOUD SECURITY ISSUES
Cloud computing model offers several appealing benefits to organizations all over the world. Making the move to the cloud offers cost savings to organizations, who previously were managing their own data centers. Most importantly, cloud computing cuts the initial hardware and infrastructure investments, and offers elasticity, meaning that organizations can react to increases or decreases in customer demand by provisioning more resources or releasing excess resources at the time of need. A cloud consumer never pays for resources that are not used.

However, making the move to the cloud often means that the control over security no remains in the hands of the customer, but in the hands of the cloud service provider. Nowadays, when we think about where an organization’s value lies in, we think about data. And yet, by making the move to the cloud the customer relinquishes the control over their data to the cloud service provider.

Organizations must ask themselves questions such as “How can I be sure that my data is secure?” and “How do I know that my data will be available to me when I need it?”

Cloud computing has transformed businesses dramatically, but at the same time in cloud computing imposes some new security issues that the cloud consumers and service providers need to tackle together. A recent survey by North Bridge [14] shows that only 50% of the 785 answerers, consisting of both cloud vendors and cloud consumers have complete confidence over cloud computing. 12% say that cloud computing still needs to mature...
especially in the security and compliance areas. Among the top reasons inhibiting adoption of cloud services are listed security (the top reason), regulatory compliance, cloud lock-in and interoperability, and privacy. Similar results can be seen in Trend Micro’s 2012 global survey on cloud security [16].

3.1 Shared Platform and Infrastructure Security
Due to the multi-tenant nature of cloud computing the platform introduces some security issues specific to cloud computing. A group of researchers have shown that it is possible to achieve virtual machine co-residence in Amazon EC2, one of the most popular public IaaS services [1]. The researchers were able to build a map of the EC2 infrastructure and using that map, they were able to achieve co-residence with possible target victim virtual machines in 40% of the time. As the control of hypervisors resides always with the cloud service provider, the cloud consumer does not have much say in the problem. By achieved co-residence an attacker can then take advantage of the target machine via covert channels by stealing cryptographic keys.

Virtual machine images shared between cloud consumers often contain flaws that may lead to leakage of private data or virtual machine hijacking. In Amazon EC2, cloud consumers can share their Amazon Machine Images, or AMIs, to other cloud consumers. A research [2] showed that a large number of shared AMIs contained remnants of AWS (Amazon Web Services) API keys, SSH keys and even private data from the creator of the AMI. The remnant SSH keys created a possible SSH backdoor to whoever possessed the corresponding private key. This was usually the creator of the AMI, who had shared that specific AMI via Amazon Cloud App Store.

Often, cloud consumers have no way of determining whether the computations and communication performed by virtual machines and the applications deployed on top of them in the cloud can be trusted, as opposed to a situation where the application is running on a user’s own computer. In the latter situation the user can possibly even fetch the source code of the application he or she is running to verify that the application really performs as advertised. Vulnerabilities in a hypervisor managed by the cloud service provider may lead to compromise all the virtual machines deployed on that virtual machine. A cloud consumer often has no other option but to trust the services provided by the cloud service provider or to not use those services.

3.2 Cloud Vendor Lock-in
One problem with cloud computing is the lack of standardization. Cloud computing services provided by different cloud service providers vary from each other, and often cloud consumers become dependent on the application programming interfaces of their cloud service provider. This situation is referred to as cloud vendor lock-in, because it “locks” the cloud consumer to continue using the services of a single cloud service provider unless the cloud consumer is willing to re-engineer its cloud-based services and data to support another cloud vendor.

This issue leads to another possible issue if the customer applications deployed on the cloud wish to communicate with services deployed on another cloud vendor’s cloud.

Different cloud service providers have different policies and specifications, which reflects to the way the service components communicate with each other. Even basic cloud functionalities such as provisioning may vary between cloud vendors. [17] recognizes service naming and location, different technologies and operation ordering mismatch as the main component-to-component mismatches. The three mismatches are similarly a part of component-to-cloud mismatch, accompanied by SLA related requirements, and cloud-specific performance services.

3.2.1 Component-to-cloud mismatches
Application service naming will vary between cloud service providers. Even in component-to-component situations the names and services a component uses will change. Hence, any non-cloud components must be designed in a way that enables them to access the components in the cloud [17].

Different technologies used to implement the cloud application programming interfaces (APIs) are one for the reasons for cloud vendor lock-in. Such technologies include Java RMI, REST, and SOAP.

Even generic operations such as the HTTP GET operation can be implemented differently between cloud service providers; the number of operation invocations and the order of those invocations may vary from a cloud service provider to another.

In addition, each cloud service provider will establish SLAs in their own way and this can have a direct impact on service components, which are expected to comply with the SLAs and application specific quality of service (QoS) requirements.

3.3 Data Security
In cloud computing applications are deployed in a shared network. Therefore confidentiality, integrity, and availability – the three cornerstones of information security – are major issues to cloud consumers [30, 16, 14]. Data confidentiality assures the cloud consumer that their data residing in the cloud can only be accessed by authorized personnel. Data integrity assures the cloud consumer that their data remains untampered and uncorrupted during storage and transit. Last, data availability implies that the data will be available when needed.

Customer data is often stored encrypted, but this data must be decrypted for any computation to be made possible on it. This means that the data is not always secure in the cloud and usually cloud consumers have little control over this issue. It is the responsibility of the cloud service provider to implement security measures to protect the customer data when it is used for computational means, and also when the data is at rest in storage.

Cloud service providers might not offer transparency to the methods they use to store customer data or to the methods they use to dispose of the data. If the cloud provider does not dispose of customer data or its storage hardware properly, the data might become exposed to other cloud consumers or even total strangers, if they can get their hands on disposed hard drives.

One of the biggest issues with cloud computing security is that cloud consumers fear that they lose control over their data when moving into the cloud. By definition, cloud computing is an abstraction and specifics about the infrastructure or security measures should not be made visible to the cloud consumer. In reality, however, organizations are often required to be able to prove that they are compliant to regulatory or legislative requirements imposed by either their customers of government laws. With the lack of transparency in the cloud it is often impossible to gather evidence on actions performed on a customer’s data. Such forensics data might be required by the
customer to prove that it is compliant to certain requirements imposed on it by a third party.

3.4 Regulatory Compliance
Two of the most common regulations that organizations need to comply to are the Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standard (PCI DSS). By transferring the control over their services and data, the cloud consumers must ensure that the cloud service provider they are using is compliant to requirements imposed on by regulations such as PCI DSS and HIPAA. Failure to prove compliance to these regulations may lead to serious penalties, and therefore simplify the risk of such penalty due to the cloud service provider being unable to comply with the regulations may be enough to inhibit cloud deployment in some organizations.

Risks exposed to the cloud consumer when making the move to the cloud are for the most part related to data security. For example, since by definition cloud offers an abstraction of the location of the data, how can you be sure that your data is stored within the borders of a certain state or country? If a healthcare organization based in the European Union stores its data on US-based servers, will that data be under the jurisdiction of HIPAA or the European regulation Data Protection Directive (DPD)?

These regulations also often require that an audit is performed, possible by a third party, from time to time. In practice, this can be cumbersome given that the data may reside almost anywhere and that the auditing of such data would require either that the auditors access the cloud service providers premises or that the whole data be transferred over the network for auditing purposes. The amount of data can be very large, which would lead to large I/O costs to the cloud consumer being audited.

4. ADDRESSING CLOUD SECURITY

4.1 Shared Platform and Infrastructure Issues
A number of solutions for mitigating and eliminating shared platform security issues have been proposed over the years. [5] and [9] describe frameworks for deploying intrusion detection systems (IDS) in the cloud. By protecting each guest virtual machine with a host-based intrusion detection system (HIDS), one can significantly reduce the risks of various attacks towards applications and infrastructure. There are already offerings available in the market for protecting virtual machines with intrusion detection and prevention, firewall and anti-malware features [16]. These solutions do not require an agent component to be installed on the virtual machines, but instead take advantage of VMware vShield Endpoint to secure the virtual machines. All traffic is routed through a special virtual appliance that performs security functions such as deep packet inspection and firewall functionality. By securing virtual machines with host-based firewalls and intrusion detection and prevention, one can mitigate the impact of attacks such as denial of service (DoS) attacks and other internal and external attacks.

Another broadly covered research topic on securing the cloud infrastructure is Trusted Computing Groups Trusted Computing. Several papers ([7],[8],[11]) discuss the use of virtualized Trusted Platform Modules (TPM) as an enabler of trust in the cloud. The use of cryptographic functions provided by the Trusted Platform Module and the TCG Software Stack (TSS) [24] enable cloud consumers to remotely attest cloud service provider to determine whether the services provided by the cloud vendor can be considered trusted.

A TPM contains an endorsement key (EK), which is a private key that identifies the TPM. The manufacturer of the module signs the corresponding public key that guarantees the correctness of the module and validity of the endorsement private key. Using other cryptographic keys provided by the TPM it is possible to sign communications, and to remotely attest the platform containing the chip using the Attestation Identity Key (AIK) pair. Remote attestation can be used to verify the integrity of the platform and it can even be used to verify which components are loading at boot time. This is possible due to measurements that compose lists of hashes from the components involved in the boot sequence of the platform. This functionality can be used to detect malware such as rootkits.

[11] proposes a trusted cloud computing platform (TCCP) that guarantees the confidentiality and integrity of a cloud consumers virtual machine. To be considered trusted, a node must be running a trusted virtual machine monitor (TVMM) and be located inside the security perimeter of the cloud service provider. It is also stated that it is important that the trusted coordinator (TC), which coordinates all the nodes and the TVMMs running on those nodes, be managed by a trusted third party, thus excluding the possibility of rogue cloud service provider admins from accessing and tampering with the trusted coordinator. [25] proposes that the third party, or external trusted entity (ETE), should have as little as possible to do with the cloud service provider.

4.2 Addressing Vendor Lock-in
Cloud vendor lock-in is a direct result of lack standardization in cloud computing. Therefore the most straightforward answer to the problem would be to enforce standards regarding cloud APIs. GoGrid API [30] is one example of a cloud API available under a Creative Commons Sharealike license.

However, it is unlikely that open APIs such as GoGrid will become the de facto norm in the industry. An API acts, by definition, as an interface into software. Therefore it is impossible to solve cloud vendor lock-in issues by only making the APIs available under licenses such as the Creative Commons license. If the software engine beneath the API is not identical in every cloud, neither will be the service regardless of the API.

Moreover, cloud vendors are unlikely to agree on a common API in the near future. Cloud service providers such as Amazon will most probably see it difficult to agree on a common API unless it is the one they invented, as they are already industry leaders among cloud service providers.

4.3 Enhancing Data Security
As data security is the number one concern in cloud security, it is also maybe the most widely researched field of cloud computing security. [3] introduces a control mechanism for propagation of sensitive data to the cloud. The implementation is based on the realization that most cloud services transfer data over HTTP protocol. The proposed solution, CloudFilter, binds data propagation policies to the files by embedding the files with XMP (Extensive Metadata Platform) labels containing information about the security policy that needs to be enforced on that specific file. The implementation makes use of proxy servers that are placed on the edges of the
customer and service provider networks. Security policies are stored in the proxies and they propagate data based on those rules. Therefore, file propagation can be tracked and controlled based on factors such as target and source domains, data classification, users and even certain keywords contained inside the file.

Another two research areas are Proofs of Retrievability (PoR) [18, 19, 20] and Proofs of Data Possession [21]. These are methods for verifying that data is stored where it is supposed to be stored and that the integrity of the file is intact. Data integrity and availability can be verified without these methods, but it requires that all the data that is to be verified is transferred over the network to the verifier or auditor. As cloud consumers pay for used bandwidth in cloud computing environments, this is not an option unless the size of the data to be verified is very small. To make PoR possible authentication tags need to be attached to each file block. The cloud consumer only has possession of the keys that are used to generate these authentication tags, and therefore only the authentication tags of each block need to be transmitted to the cloud consumer for him or her to verify the integrity of the data stored in the cloud.

Also, [31] presents a method for verifying the geolocation of the data in the cloud. This can prove useful to organizations that have regulatory or legislative requirements on the location of their data. While data is at rest, it is usually stored encrypted. However, performing computations using that data as input exposes the data for the duration of the computation. For long the ability to perform computations on encrypted data was thought to be impossible to implement, until [23] introduced the concept of fully homomorphic encryption (FHE). FHE, however, is till maturing and [22] shows that FHE cannot solve all problems, namely in multi-client settings where computing is performed across data that is supplied by multiple clients, and the results of that computation is to be revealed to multiple clients in a privacy-preserving manner.

### 4.4 Enforcing Regulatory Compliance in the Cloud

There exists guidance and frameworks to support the cloud deployment of applications that need to work under regulatory compliance. For example [25] presents guidelines for achieving PCI DSS compliance in the cloud.

The guidelines explain how responsibilities regarding PCI DSS shift towards the cloud service provider and we move from IaaS to Saas. In SaaS computing most of the responsibility is with the cloud service provider. However, the cloud consumer is not without responsibility: identity and access management must be managed together with the cloud service provider, and the cloud consumer must still adhere to its own security policies. The more technical aspects are the responsibility of the cloud service provider. These responsibilities include installing and maintaining firewall configuration, and keeping anti-virus software up to date. One interesting part of the PCI DSS regulation is that access to all network resources and cardholder data must be tracked. One efficient way of doing this is to deploy a security event and information management system (SIEM), which stores all log data on a centralized log depository, and enables reporting and incident management based on the log data. SIEM systems are often quite expensive and require intensive deployment projects. Therefore the shift of such responsibility from the cloud consumer to the cloud service provider saves the customer both time and resources.

Some cloud vendors already offer regulation-tailored cloud computing services to customers. For example, Microsoft offers cloud services for health [26]. Microsoft Cloud Services for Health promises that health organizations retain control of their sensitive data at all times. Microsoft also promises that its data centers are certified for Federal Information Security Management Act (FISMA), ISO/IEC 27001 information security management system (ISMS) standard and SAS 70 Type II auditing standard.

However, some legal regulations such as HIPAA demand that the outsourced data must not be leaked to external parties, such as third party auditors (TPAs). To solve this problem, [12] presents a privacy-preserving public auditing system for data store security in the cloud by utilizing homomorphic authenticator and random masking, which guarantees that the third party auditors will learn no knowledge about the audited data.

### 4.5 Addressing additional cloud security issues

A recent listing of top threats to cloud computing named “The Notorious Nine” [27] by Cloud Security Alliance (CSA) lists nine top threats to cloud computing, voted by industry experts. These top threats include data security issues such as data breach and loss, account hijacking, insecure application programming interfaces, denial of service attacks, and shared technology issues. The document published by CSA also gives guidelines to controlling these threats.

According to CSA, data breaches were ranked as threat number five in 2010, but are ranked as number one threat in 2013. Controls for addressing this issue include secure disposal of data, encryption and identity and access management.

Account or service hijacking is said to result partly from the reuse of credentials and passwords. The threat is also increased by phishing and exploitation of software vulnerabilities. Controls to address account or service traffic hijacking are highly related to an organizations information security management system, and namely their user access policies. Multi-factor authentication may mitigate the threat and audit logging and intrusion detection will help gather evidence for digital forensics.

Threats from malicious insiders are one of the threats in the listing that has gone down in the ranking since 2010. Similarly to data breaches, data access from malicious insiders can be prevented by implementing strong encryption, identity and access management policies and maintaining facility security on the cloud service provider’s premises.

Previously a number one threat and now only seventh in the listing is the abuse of cloud services. As cloud computing is relatively affordable, it presents a possibility to criminals to rent out cheap computing resources to stage a distributed denial of service attack (DDoS) or server platform from where to serve out malware or pirated software. Controls for addressing this issue include incident response processes and acceptable use policies.

Attacks towards web services remain to be one of the persistent threats towards cloud services as these services are accessed through the internet. The latest of OWASP’s top 10 report [28] lists SQL injection attacks as the number one threat to web applications. A full list of the OWASP Top 10 can be seen in the 2013 release candidate. All of these threats come to play at least when IaaS or PaaS customers deploy their own applications to the cloud. Needless to say, security must already be made part of the
software design process: security needs to be built into the software, not glued on top of it.

4.6 Security Event and Information Management Systems

A subject that has received fairly little focus on academic research papers is the use of Security Event and Information Management (SIEM) systems for tackling security issues in the cloud.

To put things coarsely, a SIEM system is a log management system with extended abilities to do analysis and reporting on the gathered log data. A SIEM system feeds on logs generated by network devices, operating systems, applications, and almost everything that has the capability to produce logs. This log is either pushed or pulled into the SIEM system, and this log data can be used to generate alerts based on rules and heuristics, and it can also be used to generate scheduled reports on many subjects, such as failed logins by user, inbound or outbound traffic blocked by a firewall, or even IDS alerts. Alerts are then correlated by the correlation engine, meaning that related alerts originating from devices such as firewalls, intrusion detection sensors and web servers are correlated into a single alert, which reduces the work of the employee who has to analyze the alerts.

Other features supported by a traditional SIEM system are out of the box support for a vast amount of log sources (device types and applications) and guarantee that the log data stored by the SIEM system remains untampered with, as one of the major reasons for the existence of SIEM systems to begin with are regulations such as PCI DSS, which dictates that access to all network devices and cardholder data must be monitored. In fact, Sarbanes-Oxley (SOX) is the biggest reason SIEM systems exist today. The SOX regulation requires that event management be made a core component of the control framework described in ‘Sarbanes Oxley section 404 [33].

If a SIEM system can do all this, why is it not part of every organization’s IT infrastructure? First of all, enterprise-grade SIEM system are rather expensive, and not many SIEM product fit the needs of small and medium sized businesses, as licensing costs grow based on the number of monitored host in the hundreds, not in the tens. Also, deploying a SIEM system can be a devious task and often requires a project and hours and hours of professional work. Log sources need to be mapped and configured, SIEM log parsers and normalizers might need customizing if the environment includes some of the more exotic device types or applications. In addition, reports need to be customized based on the customer’s needs. And when the system is up and running, it usually needs to establish a baseline of traffic and user activity for it to be able to produce alerts based on deviations from actions or traffic patterns that are considered normal or safe. This period probably also involves a lot of false positives, which need to be weeded out to increase working proficiency.

But then the SIEM has matured in the customer environment, it starts to produce valuable output about security incident, violation of company policies, misconfigured systems etc. Reading the alerts might be easy for your ordinary organization IT department guy, but deeper analysis after the alert usually requires skills of a security analyst. Therefore SIEM systems work wonders when coupled with professional security analysts or a security operations center (SOC), which handles security incidents. Also, large organizations might consider building a security incident response team (SIRT) to tackle the most critical incidents.

The author personally thinks that implementing SIEM systems in the cloud might help to address most of the issues related to regulatory compliance. Also, the reporting capabilities of a SIEM system could be used to offer customer transparency to the security of the platform they are using. This could help reduce the fear of the cloud and also give cloud consumers a sense that they have not relinquished all of their control over their data.

5. CONCLUSION

This survey shows that the amount of threats concerning cloud computing is large and the set of threats is heterogeneous. However, there exist a lot of solutions and proposals on how to address these issues. It must be noted that the responsibilities of implementing security measures depends largely on the service model used. SaaS customers will see that most of the responsibility is on the cloud service provider, and therefore customer must choose their cloud vendor based on the security offered by the service provider and risk analysis must be conducted to address issues that remain uncovered by the cloud service provider. As an opposite, IaaS customers have more responsibilities over the security of their platform, but therefore also have more freedom and more saying in how security is implemented.

Actors such as Cloud Security Alliance and PCI Security Standards Council offer guidelines on how to address security and regulatory issues in the cloud. The Cloud Controls Matrix (CCM) [32] by Cloud Security Alliance offers security principles targeted towards cloud vendors and cloud customers. The CCM provides a controls framework and gives out detailed information regarding principles and practices concerning cloud computing and different regulations and standards, such as ISO 27001 and 27002, PCI DSS.

There exist a variety of solutions that can be implemented to enforce data security. These solutions include data encryption to enforce data confidentiality, Proof of Retrievability and Proof of Data Possession to enforce data availability and data integrity, and measures for secure data propagation to the cloud using labels embedded in the data.

Shared platform issues can be addressed by securing the virtual machines with host-based firewalls, intrusion detection systems and anti-malware software. With current market offering, such protection of virtual machines can be achieved without the need to install an agent to the virtual machines, therefore reducing the load imposed on a protected virtual machine. The implementation also ensures that virtual machines are protected immediately after they are started.

The use of trusted computing and virtualized trusted platform modules enables customers to attest the cloud service provider’s platform to verify that the virtual machines are running only acceptable software. In the same way, the cloud platform can verify the cloud consumer by attesting the customer host.

Fully homomorphic encryption is showing some promising results, which will perhaps someday lead to wide adaptation of this encryption scheme were data needs not to be decrypted while it is used for computation. Similarly it offers benefits for audits performed by third party auditors, as some regulations such as HIPAA do not allow the sensitive data to be revealed to third party auditors.
6. REFERENCES


