Paper Summary

The architecture of cloud computing consists of the interconnection of different distributed systems and their usages. Many organizations have started using cloud technologies in this decade. But cloud computing is vulnerable to various kinds of privacy issues and malware attacks which creates a need for a strong identity and access management mechanism. The paper discusses the issues related to authentication, access management, and security, and the techniques to overcome these issues. IAM in the cloud environment is a very important factor while migrating to cloud service. Lack of efficient mechanism in IAM will create multiple challenges like identity management, risk management, data security, privacy, data leakage, and transparency. Cloud service providers are responsible for these managements and they must ensure that data and applications are protected, and the infrastructure is secure. IAM systems perform different operations for providing security like authentication, authorization, storage, and verification provisions, the security of identity. There are many different types of authentication mechanisms are physical security mechanisms(access cards and biometrics), digital security mechanisms (credentials, SSH keys, multifactor authentications), PIN (asymmetric encryption technology), SSO (one password for all cloud applications). SSH keys are not better if the private keys are not secured whereas their advantage is authentication is performed without passing the password. There are many types of SSO methods are Enterprise SSO (maintaining session cookies), OpenID (the open standard protocol that allows user's authentication to the relying parties), OAuth (one way or mutual way authentication), SAML(works on token-based request-response services). There are different types of authorization mechanisms for access control are MAC, DAC, RBAC, ABAC. MAC permits OS or kernel which are set by system managers, DAC controls permissions through data owner, RBAC provides access rights based on roles and privileges of users, and ABAC defines access control by use of policies. Identity and access management authenticates users, devices, and services and provides rights to grant or deny data. It controls access to resources based on predefined policies. IAM also does Authentication management and manages the password and digital certificates. SPML is a framework used for identity management in IAM. After authentication, IAM manages authority and ensures that the resources are secure and accessed concerning the policies. Privacy and interoperability are the main issues in existing IAM approaches. Many organizations such as IBM, Oracle, RSA, SailPoint provide the IAM system to secure the information by controlling access permission of the users. Each organization uses different ways and techniques to achieve the best possible security and uses a variety of myriad solutions. Threats in the cloud infrastructure include data security, virus, availability of resources, and multitenancy. Due to the increased processing capacity of devices, security is mostly compromised using a brute-force attack. Viruses spread to all the users of the cloud if one user gets malware on their local system. The availability of resources is impacted in the event of a security breach. There are many different threats and attacks possible in cloud services discussed thoroughly in the paper and proper precautions should be taken for it

My views: Cloud computing is one of the most important area for data storage and processing, but there are scopes of vulneraries. IAM plays a major role in managing the security of resources. While using the cloud services, we can keep some aspect in our mind such as Multifactor authentication, SSH should be used. ABAC mechanism to be used to create specific policies for specific resources while working on different cloud services.