ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020

Enhanced Password-Based User Authentication Using MFA

Preeti Kushwaha[1], Prof. Satpal Singh[2]

M.Tech. Scholar, Department of Computer Science &Engineering, Global Engineering College, Jabalpur, Madhya Pradesh, India[1]

Assistant Professor, Department of Computer Science &Engineering, Global Engineering College, Jabalpur, Madhya Pradesh, India[2]

ABSTRACT: Cloud is a forthcoming revolution in organizations because of maintaining different services like SaaS, PaaS, DaaS, laaS for public and private users of information technology. To avail these services in an effective and efficient way users have to legalize with cloud service providers (CSP). In this process CSP requires highly secure authentication scheme because attackers are becoming more cosmopolitan. This paper proposes a strong authentication scheme by using Multi Factor Authentication Protocol (MFA) along with two factor authentication (OTP). The first password is used to verify the profile of a user and second is used to provide access to the services of cloud. Additionally,

KEYWORDS: Multi-factor Authentication(MFA), StaticPassword, Time-based OneTime, Passwords (TOTP) andQuestions based Authentication.

I. INTRODUCTION

In the world of computer science, during the 60s and 70s, the computation has been done by client-server architecture (Centralized Computing). This technology has been changed to distribute computing with the development of computing technologies. However, nowadays, the computing technologies again going back to the virtual centralized computing (Cloud Computing). The cloud computing concept was first proposed by Eric Schmidt in 2006.Cloud computing model allows access to information and computer resources using a delivery of computational services (e.g. Online le storage, social networking sites, webmail and online business applications) which allows to access software and hardware that are managed by a third party at remote locations.
The following definition of cloud computing is given by NIST: "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. Networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management e ort or service provider's interaction and has been developed very quickly in the recent years [6]." This new paradigm came up with essential characteristics, service models and deployment models.

1.1 Service Models [6]:

Infrastructure as a Service (IaaS): The consumer is able to deploy and run any application onto the fundamental resources which is provided by IaaS providers. This model has lowest service abstraction and highest resource visibility. The consumer has control over operating system and application, but doesn't have control over the underlying cloud infrastructure. Example: Amazon AWS [6] [9].
Platform as a Service (PaaS): This model provides a platform to the developer to develop and deploy applications onto the cloud infrastructure by providing programming construct and tools, which can be supported by the providers. This model provides higher service abstraction than SaaS and lower resource visibility than SaaS. Deployed

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020

applications can be controlled by a consumer, but has no control over the underlying cloud infrastructure. Example: Google App Engine [6] [9].

Software as a Service (SaaS): Service providers deploy services to the web which provides remote access to the end user for accessing capabilities. The end user can utilize these services through the web interface. This model provides highest service abstractions and lowest resource visibility. This model hides the implementation of the application to the consumer. Services and underlying cloud infrastructure are not managed or controlled by the consumer. Example: gmail.com [6] [9].

1.2 Deployment Models [6]:

Public cloud: The cloud infrastructure is available to the general public with shared purpose which can be owned or managed by third parties who are providing cloud services.

Private cloud: The cloud infrastructure is managed or controlled by the particular organization or third party which is operated for particular an organization [9].

Community cloud: The cloud infrastructure is shared by several organizations for particular concerns like mission, security requirements, policy which can be owned or managed by third parties or the organization [6].

Hybrid cloud: An organization can use the combination of any two or more of the above models to cloud deployment for taking advantages of individual deployment model.

Security is one of the major issues in cloud infrastructure for adapting the cloud computing technology in IT industries. In cloud computing paradigm, the third party is providing processing capabilities, space for storing information, support for services, etc. Many organizations are storing their crucial information in the cloud database in a cloud environment. Third party maintains the cloud database. The user has to prove their identity to the service provider for seeking.

1.3 The verification process has been done by one of the three types of confirmations:

Something known: Secret thing is only known to the user that can be verified by the service providers. Examples are pin no, password, private key.

Something possessed: Something that verifies the users' identity. Examples are ATM card, drivers' license, smart card.

Something inherent: Something that is inherent properties of a user. Examples are fingerprinted, retina scan, and voice.

There are three major techniques for authentication:

Password based authentication: The oldest and simplest method of authentication for accessing the resources in which user has to provide a password which is only known to the user.

Challenge-Response authentication: In this technique, users have to prove that they know the secret without sending it to the service provider. The challenge is any time stamp value which is sent by the service provider and user applies a function on challenge to send response to the service provider.

Zero-Knowledge authentication: In this technique, the user does not disclose anything that might take a chance to the confidentiality of the secret. The user proves to the service provider that they know the secret without disclosing it to the service provider. User and service provider exchanges some messages to each other for authentication. After exchanging these messages, service provider somehow knows that the user knows the secret.Single-tier authentication can be implemented using one these techniques, but still single-tier authentication is not enough to secure the resources of the service providers in a cloud environment because this technique is suffering from many security attacks like, brute-force attack, insider attacks, in a cloud environment. For making more secure authentication model, the researcher came up with multi-tier authentication.This new technique leads to less probability of breaking the authentication system which provides more security to the resources of the cloud providers. The multi-tier authentication technique uses two or more verification process to verify the user.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020

II. LITERATURE REVIEW

This chapter introduces the single-tier and multitier authentication techniques and study related to its security analysis for strengthening the existing authentication techniques. It also describes the study about existing authentication techniques and its deficiencies with respect to cloud environments.

2.1 Review of different authentication techniques

A Secure Multi-Tier Authentication Scheme in Cloud Computing Environment, Ashish Singh, KakaliChatterjee

Ashish Singh, KakaliChatterjee proposes a secured and more advanced multi-tier authentication scheme for accessing cloud services. Multi-tier authentication scheme is much more secured than single-tier authentication scheme. This paper proposes a multi-tier authentication scheme in which single-tier authentication is not sufficient for accessing the services. The authentication process is done in two steps (two-level). In the first step, user enters simple username and password. In the second step, user The second-tier authentication is based on a sequence of predetermined activity of user on screen. Advantage of this two-tier authentication scheme has no need of any extra hardware and software. This paper presents the design and implementation of a secure multi-tier authentication scheme in cloud computing. This paper proposed limitations of existing authentication technology and shows the comparison of various techniques based upon the some parameters. The proposed scheme provides a balanced solution between the security and performance. Changing the username and password in both the tiers do not possible. This is major concern and has to be taken care of in future. The other possible ways of recovering the passwords in multi-tier environment are the possible future improvements.

Secured Cloud Architecture for Cloud Service Provider, Mr.Nilesh R. Patil ,Prof. Rajesh

Mr.Nilesh R. Patil , Prof. Rajesh proposed the secure architecture for cloud which is going to map some cloud security issues that are authentication of user, confidentiality, privacy, access control and checking the integrity of data. For authentication of user system uses One Time Password (OTP), for data integrity check system uses modified SHA-2 hash function. This modified version of SHA-2 will provide better solution for PreImage attack and Collision attack and for encryption and decryption system uses standard Advanced Encryption Standards (AES) algorithm. The proposed cloud architecture is more efficient because it uses efficient hashing algorithm which maps the Preimage attack and Collision attack. Future work proposed in this paper will design hashing algorithm for Media files such as audio, Video, Images etc.

Multi-Factor Authentication as a Service Andreas, U. Schmidt, LakshmiSubramanian

Andreas U. Schmidt, Lakshmi Subramanian proposed an architecture for providing multi-factor authentication as a service (MFAaaS).The proposed architecture is robust and scalable. They have presented architecture for a unified approach to user authentication in the spirit of cloud services. The MFAaaS aggregates authentication factors and exposes them to services. A modular architectural approach makes the system lightweight and follows the principle of separation of duties. Security and privacy are major concerns for centralized services such as the MFAaaS. On the other hand, the MFAS separates the duties between SP and Auth Servers, so that authentication factor providers cannot gather information about SP access by users, and, *vice versa*.

MITM attack

A man in the middle (MITM) attack is a general term for when a perpetrator positions himself in a conversation between a user and an application—either to eavesdrop or to impersonate one of the parties, making it appear as if a normal exchange of information is underway.

The goal of an attack is to steal personal information, such as login credentials, account details and credit card numbers. Targets are typically the users of financial applications, SaaS businesses, e-commerce sites and other websites where logging in is required.

Information obtained during an attack could be used for many purposes, including identity theft, unapproved fund transfers or an illicit password change. Additionally, it can be used to gain a foothold inside a secured perimeter during the infiltration stage of an advanced persistent threat (APT) assault. Broadly speaking, a MITM attack is the equivalent

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

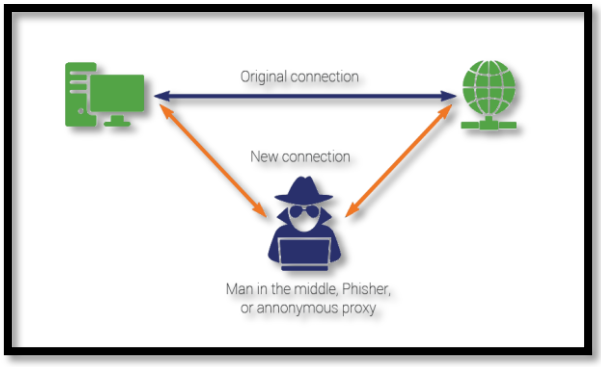
International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020

of a mailman opening your bank statement, writing down your account details and then resealing the envelope and delivering it to your door.



Man in the middle attack example
MITM attack progression
Successful MITM execution has two distinct phases: interception and decryption.

Interception
The first step intercepts user traffic through the attacker's network before it reaches its intended destination.
The most common (and simplest) way of doing this is a passive attack in which an attacker makes free, malicious WiFi hotspots available to the public. Typically named in a way that corresponds to their location, they aren't password protected. Once a victim connects to such a hotspot, the attacker gains full visibility to any online data exchange.

Attackers wishing to take a more active approach to interception may launch one of the following attacks:
IP spoofing involves an attacker disguising himself as an application by altering packet headers in an IP address. As a result, users attempting to access a URL connected to the application are sent to the attacker's website.

ARP spoofing is the process of linking an attacker's MAC address with the IP address of a legitimate user on a local area network using fake ARP messages. As a result, data sent by the user to the host IP address is instead transmitted to the attacker.

DNS spoofing, also known as DNS cache poisoning, involves infiltrating a DNS server and altering a website's address record. As a result, users attempting to access the site are sent by the altered DNS record to the attacker's site.

Decryption
After interception, any two-way SSL traffic needs to be decrypted without alerting the user or application. A number of methods exist to achieve this:

HTTPS spoofing sends a phony certificate to the victim's browser once the initial connection request to a secure site is made. It holds a digital thumbprint associated with the compromised application, which the browser verifies according to an existing list of trusted sites. The attacker is then able to access any data entered by the victim before it's passed to the application.

SSL BEAST (browser exploit against SSL/TLS) targets a TLS version 1.0 vulnerability in SSL. Here, the victim's computer is infected with malicious JavaScript that intercepts encrypted cookies sent by a web application. Then the app's cipher block chaining (CBC) is compromised so as to decrypt its cookies and authentication tokens.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020

SSL hijacking occurs when an attacker passes forged authentication keys to both the user and application during a TCP handshake. This sets up what appears to be a secure connection when, in fact, the man in the middle controls the entire session.

SSL stripping downgrades a HTTPS connection to HTTP by intercepting the TLS authentication sent from the application to the user. The attacker sends an unencrypted version of the application's site to the user while maintaining the secured session with the application. Meanwhile, the user's entire session is visible to the attacker.
Man in the middle attack prevention
Blocking MITM attacks requires several practical steps on the part of users, as well as a combination of encryption and verification methods for applications.

For users, this means:
Avoiding WiFi connections that aren't password protected.
Paying attention to browser notifications reporting a website as being unsecured.
Immediately logging out of a secure application when it's not in use.
Not using public networks (e.g., coffee shops, hotels) when conducting sensitive transactions.
For website operators, secure communication protocols, including TLS and HTTPS, help mitigate spoofing attacks by robustly encrypting and authenticating transmitted data. Doing so prevents the interception of site traffic and blocks the decryption of sensitive data, such as authentication tokens.
It is considered best practice for applications to use SSL/TLS to secure every page of their site and not just the pages that require users to log in. Doing so helps decreases the chance of an attacker stealing session cookies from a user browsing on an unsecured section of a website while logged in.'

III. PROPOSED SCHEME

We made some modification to the authentication technique proposed by Singh, Maninder, and Sarbjeet Singh et al. [5] to overcome the problems in the existing technique. We proposed an authentication technique by modifying the existing two-tier authentication model to three-tier authentication with including the one extra authentication factor for verifying the intended user to overcome the insider attack and providing single-sign on access of the registered services.
The proposed authentication technique works on three phases. In the first phase, the users register themselves with the first-tier and second-tier and third-tier authentication credentials. The first-tier authentication credentials are simple like username and password whereasin the second-tier authentication. We are using the email secret code as the second-tier authentication code. This secret code is valid for some amount of time to access the requested service. We provide the time limit with the secret code. After the time limit expires, the user can not access the requested service with that secret code. The user needs another secret code for accessing the requested service.For The third-tier authentication credentials are like pattern matching or text field activity like in the existing technique [5].

We took the pattern matching as the third-tier authentication credentials to simulating the proposed scheme.The figure 3.1 shows the abstract model of the proposed multi-tier authentication technique for single-sign on (SSO) access of cloud services.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020

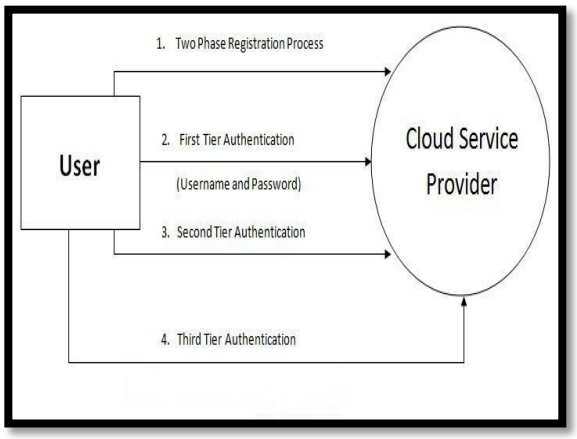


Figure 3.1: Abstract design of proposed authentication model

In the first tier, the proposed model verifies whether the intended user or not. After the first phase, the second-tier credentials are used to authorize the requested user by providing the one time secret code to the authentication system. This one time secret code is send to user email id. Finally, the third-tier authentication credential is used to authenticate the requested user again and provide the access the requested service.

The proposed scheme follows the following steps to authenticate the user for accessing the requested services.
1. To get access in cloud application, first user needs to pass username and password.
2. In the second-tier, Email based One Time Password must be entered.
3. In the third-tier, user need to answer Knowledge based security question.

IV. IMPLEMENTATION

To solve the problem of secure authentication, we are using the concept of multi tier and multifactor authentication. In the proposed security model one time password has been used with user name and password for authenticating the user. Along with these credentials, we are using set of random questions; these questions are based upon the user's activities on web. User has to give correct answers for authenticate themselves and for getting the access.

The user sign up process starts with first tier user authentication process, user sign up interface where the user enters its static username and password details. This information moves for verification to the system's database. Once it is verified, the system generates one time password for next level authentication. This OTP is sent to user's registered email account. The OTP is valid only for 2 minutes time. The one time password is time synchronized with both the end. The session value is also attached with this OTP for better security. In next event, user has to reply with their email OTP within given time limit. If user is unable to reply with OTP within time limit, then user can request new OTP from the System.

Ones user validates two levels of authentication, system continues with next tier authentication process. In this, system generates set of five questions randomly from their database; user has to give four correct answers of the set of questions. User has to give all the six correct answers within 2 minutes of time. For this level authentication, there will be two scenarios can occur:

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020

i. User's time limit expires.
ii. User replies less than six correct answers.

In both the situations, user has three attempts for authentication. If user unable to authentication using three attempts, complete authentication process will start from the beginning.Each correct answer generates a score called API score. If user's API score is greater than four, then user authentication will be successful. If user API score is less than six,then user's authentication will be failed. At this level, if user authentication fails, then the complete authentication process will restart from tier one level. If user succeeds to authenticate, then user can access services from service provider.

V. RESULT AND COMPARISON

5.1 Security Analysis

The proposed authentication technique uses three phases of authentication. First phase used to verify using the password, second phase authorizes the user using pattern matching and finally the user authenticated with the secret code.

Let Success (S) and Failure (F) be the two outcomes of the requested cloud services.
So, the outcomes of the three authentication levels are SSS, SSF, SFS, SFF, FSS, FSF, FFS, FFF and N (O) = 8 for our proposed authentication model, where, O = outcomes.

Now, let, the p = probability of the success for accessing the services at each authentication level So, success, SSS, for breaking the whole authentication system, i.e. multi-tier authentication system is denoted by P (E). Where, $P(E) = p^3$. This leads the failure for breaking the authentication system is $1 - P(E) = 1 - p^3$.
Now, let say p = 0.2, then $p^2 = 0.04$ and $p^3 = 0.008$. It means the probability of success in breaking the whole authentication system is very less, almost zero, compared to one-tier and two-tier authentication system.

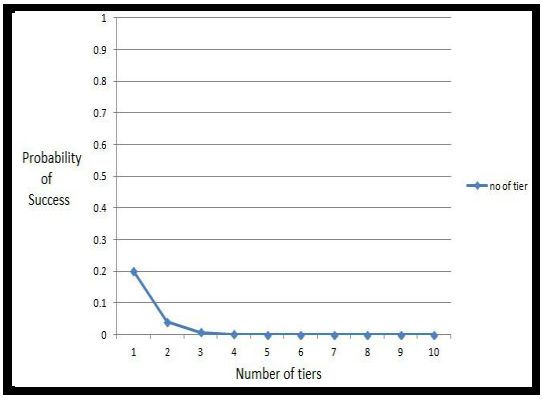


Figure 4.1 clearly shows that the probability of success in breaking the multi-tier authentication system is exponentially followed with the number of tiers in the authentication system.

Comparison between Existing Authentication Model and Proposed Authentication Model

The following table shows the comparison between existing authentication technique and proposed authentication technique with three comparison parameters.
Table Comparison between existing technique and proposed technique

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020

Comparison Parameters	Multi-tier authentication technique	Multi-tier authentication technique(Our Scheme)
Probability of success (p)for breaking the authentication system (let,p=0.1)	0.01	0.001
Additional hardware and software requirements	Yes	No
No of authentication factor	Two	Two

VI. CONCLUSION

Any authentication system's core strength depends upon the probability of success for breaking that system for accessing the services provided by the cloud service providers. In our proposed authentication scheme, the core strength is first-tier, second-tier and third-tier authentication user credentials. For getting the access of the requested service, the attacker has to break all the authentication layers.

Security analysis says that increases as the number of authentication tiers in the system, the probability of success for breaking the multi-tier authentication system reaches near to the zero. Hence, by seeing the analysis of security, we can say that there is a very less probability of breaking the multi-tier authentication system. If we consider the usability of the storage space, then the proposed technique takes more space than the existing authentication technique which is very less and also we can say that it is negligible in the case of cloud environment where large amount of storage and its scalable.

Space requirement says that the as increases the number of registered users in the cloud application, the storage space consumed by the user's credentials are linearly increases and this will not cause more processing and fetching overhead to the cloud server. For handling the pressurized situations, this technique adds the fake screen concepts. This fake screen is not related to any software and hardware.

By using the secret code on SMTP protocol mechanism, the proposed authentication technique provides the single-sign on access of the cloud services provided by the service providers. The user has to provide a secret code which is getting on the registered mail id for accessing the particular requested service.

REFERENCES

[1] Ashish Singh , Kakali Chatterjee “A Secure Multi-Tier Authentication Scheme in Cloud Computing Environment” 2015 International Conference on Circuit, Power and Computing Technologies [ICCPCT] ,©2015 IEEE
[2] Mr. Nilesh R. Patil , Prof. Rajesh “Secured Cloud Architecture for Cloud Service Provider” 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (WCFTR’16),© 2016 IEEE
[3] Yogendra Shah, Vinod Choyi, Andreas U. Schmidt, Lakshmi “Multi-Factor Authentication as a Service”, 2015 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering. ©2015 IEEE
[4] Ms. Shilpi Harnal Deepak Bagga. Single sign-on authentication model for cloud computing using kerberos. 2013.
[5]Maninder Singh and Sarbjeet Singh. Design and implementation of multi-tier authentication scheme in cloud. International Journal of Computer Science Issues (IJCSI), 9(5), 2012.
[6] Peter Mell and Tim Grance. The nist definition of cloud computing. National Institute of Standards and Technology, 53(6):50, 2009.
[7] Panagiotis Kalagiakos and Panagiotis Karampelas. Cloud computing learning. In Application of Information and Communication Technologies (AICT), 2011 5th International Conference on, pages 1{4. IEEE, 2011.
[8]Barrie Sosinsky. Cloud computing bible, volume 762. John Wiley & Sons, 2010.
[9]Rasib Hassan Khan, Jukka Ylitalo, and Abu Shohel Ahmed. Openid authentication as a service in openstack. In Information Assurance and Security (IAS), 2011 7th International Conference on, pages 372{377. IEEE, 2011.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020

[10]Davit Hakobyan. Authentication and authorization systems in cloud environments. 2012.
[11]David Chou. Strong user authentication on the web. http://msdn. microsoft.com/en-us/library/cc838351.aspx, August 2008.
[12]Federal Financial Institutions Examination Council. Authentication in an internet banking environment. 2011.
[13]William E Burr, Donna F Dodson, and William T Polk. Electronic authentication guideline. Citeseer, 2004.
[14] Ashish G Revar and Madhuri D Bhavsar. Securing user authentication using single sign-on in cloud computing. In Engineering (NUiCONE), 2011 Nirma University International Conference on, pages 1{4. IEEE, 2011.
[15] Prashant Srivastava, Satyam Singh, Ashwin Alfred Pinto, Shvetank Verma, Vijay K Chaurasiya, and Rahul Gupta. An architecture based on proactive model for security in cloud computing. In Recent Trends in Information Technology (ICRTIT), 2011 International Conference on, pages 661{666. IEEE, 2011.
[16] Wenjun Zhang. 2-tier cloud architecture with maximized ria and simpledb via minimized rest. In Computer Engineering and Technology (ICCET), 2010 2nd International Conference on, volume 6, pages V6{52. IEEE, 2010.
[17] Fengyu Zhao, Xin Peng, and Wenyun Zhao. Multi-tier security feature modeling for service-oriented application integration. In Computer and Information Science, 2009. ICIS 2009. Eighth IEEE/ACIS International Conference on, pages 1178{1183. IEEE, 2009.
[18] Zubair Ahmad, JA Manan, and Suziah Sulaiman. Trusted computing based open environment user authentication model. In Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on, volume 6, pages V6{487. IEEE, 2010.