Cloud based Secure Trust based Middleware for Smartphones for Accessing Enterprise Applications

Harsukhpal Singh
M.Tech. Computer Science
Chandigarh Engg. College
Landran, Mohali.

Mandeep Singh
Asst. Prof.
Chandigarh Engg. College
Landran, Mohali

Raman Puneet Singh
Asst. Prof.
Chandigarh Engg. College
Landran, Mohali

ABSTRACT
There are about 6,098 million wireless devices in the world and there were 117.7 million smartphone users in 2012. The number is increasing day by day. With the attractiveness of web services for mobile devices, the concern of security for mobile devices has been brought up. There is a need for organizations to allow employees to use smartphones for their work. More and more wireless Devices are being used, moreover, with more and more collaboration of organizations, web services are now in general involved with more than one organization and they use enterprise applications deployed mainly on the Cloud. The Enterprise applications are being accessed by the wireless devices and fixed connections. Trusting the wireless devices mainly smartphones is an issue with the devices. With the increase of Mobile users Mobile computing required more enhanced security than traditional computing systems.

This paper focuses on building a secure middleware based trust on the cloud. Smartphones accessing the Enterprise Applications on the cloud will have to get access as per the trust polices used by the trust models in the middleware. It resolves the issues caused by the smartphones being stolen, insecure communication between the smartphones and cloud, users misusing the privileges. The Secure middleware will be hosted on cloud platform for enhancing the security. The trust value is calculated for all http requests from the smartphones to cloud and then to decide whether the request should be served or not by the middleware. The thought of the Secure Middleware is to make the trust models more adaptable scalable and optimized for the smartphones accessing the enterprise applications.

General Terms
Cloud Computing, Distributed Systems, Smartphones, Middleware

Keywords
Middleware, Trust Models, Android, Trust policies, CloudSim, Trust Policy

1. INTRODUCTION
1.1 Introduction to Smartphones
A smartphone is a mobile phone that is proficient of doing much more than what you would conventionally expect from a phone. The finest way to think of it is that it's like having a small computer in your pocket so thatyou can do things like downloading applications, receiving and sending emails and browsing the Internet.

Most of us have heard people talking about operating systems such as Android, iOS and Windows Phone. Every smartphone uses an operating system the same way your computer at home may use windows as an operating system. It controls the phone's functions and performs tasks to keep the phone operational. While choosing a smartphone it's worth looking into the operating system the phone uses and often people will prefer a particular one. Smartphones are also able to hold a lot more memory as compared to mobile phones in the past. This means you'll be able to save more photos and videos as well as download a number of applications. The phone may also have a memory card slot so there is always space for more. You can usually see how much space you have on your phone by looking in your phone's settings. If you haven't had a smartphone before you'll notice the difference when you use one and expectantly enjoy the increased options and flexibility they provide.

As mobile network infrastructures [5] constantly improve, their data transmission becomes increasingly accessible and affordable, and thus they are becoming popular clients to consume any Web resources, especially Web Services (WS) [9]. Today, mobile devices like iPhone, Blackberry, Android, have included applications that consume WS from popular websites, such as Google, Twitter and Facebook.
On the other hand, there are problems in connecting smartphones to existing Cloud because of Security issues. Firstly, the requests form smartphones need to secure and optimization for smartphones [6]. For example, the size of the messages needs to be condensed to fit the bandwidth of mobile clients. Secondly, mobile clients have to adapt to different kinds of WS, for example, SOAP and RESTfulWS. The growing number of mobile clients and availability of WS also drives the needs of customizing the applications.

1.2 Introduction to Android
The majority of the smartphones today run on software called Android™. Android™ is developed by Google™ for mobile phones and tablets. The software contains a range of Google™ applications that come with your smartphone, like Gmail™, Google™ Search, Google Maps™ and YouTube™. Since Android™ is open-source software you can choose from a vast selection of applications to install. These applications – or apps, as they are often called – make your smartphones very versatile, as you can tailor it to suit your needs.

1.2.1 Android versions
Android™ software is constantly evolving. When a new software version is available for your smartphone, you can update it with new features and the latest improvements. New versions are free of charge. Figure 1 shows the history of Android versions.

Fig 1: Different Versions of Android.

Android™ software is constantly evolving, to give you the best experience possible. It is committed to make sure that you get the most out of your smartphone, which is why it always shares our newest software capabilities with you. Android application is being used in this thesis to communicate with the proposed middleware.

1.4 Introduction to Middleware

Middleware is the software that connects software components or enterprise applications [12]. Middleware is the software layer that lies between the operating system and the applications on each side of a distributed computer network [7]. Typically, it supports complex, distributed business software applications. Middleware [12] is the infrastructure which facilitates creation of business applications, and provides core services like concurrency, transactions, threading, messaging, and the SCA framework [4][15] for service-oriented architecture (SOA) applications. It also provides security and enables high availability functionality to your enterprise [16].

Middleware includes Web servers, application servers, content management systems, and similar tools that support application development and delivery. It is especially integral to information technology based on Extensible Markup Language (XML), Simple Object Access Protocol (SOAP) [9], Web services, SOA, Web 2.0 infrastructure, and Lightweight Directory Access Protocol (LDAP)[11], etc.

Managing these applications and the underlying middleware technology can be difficult and IT organizations often have to rely on a variety of specialized tools. This can lead to inefficiency and may introduce complexities and risks. Enterprise Manager Grid Control is a definitive tool for middleware [12] management and allows you to manage both Oracle applications and custom Java EE applications that run on a combination of Oracle Middleware and non-Oracle Middleware software.

1.5 Introduction to Cloud Computing

Cloud computing is the next stage in the Internet's evolution, providing the means through which everything — from computing power to computing infrastructure, applications, business processes to personal collaboration — can be delivered to you as a service wherever and whenever you need.

The "cloud" in cloud computing can be defined as the set of hardware, networks, storage, services, and interfaces that combine to deliver aspects of computing as a service. Figure 2 shows the cloud services being accessed by various clients. Cloud services include the delivery of software, infrastructure, and storage over the Internet (either as separate components or a complete platform) based on user demand. Cloud computing has four essential characteristics: elasticity and the ability to scale up and down, self-service provisioning and automatic DE provisioning, application programming interfaces (APIs), billing and metering of service usage in a pay-as-you-go model. See Figure 1.4 for a typical cloud in the web. This flexibility is what is attracting individuals and businesses to move to the cloud.

Fig 2: Different devices accessing Web Services on Cloud.

Cloud computing can completely change the way companies use technology to service customers, partners, and suppliers. Some businesses, such as Google and Amazon, already have most of their IT resources in the cloud. They have found that it can eliminate many of the complex constraints from the traditional computing environment, including space, time, power, and cost.

A simple example of cloud computing is Yahoo email, Gmail, or Hotmail etc. All you need is just an internet connection and you can start sending emails. The server and email management software is all on the cloud and is totally managed by the cloud service provider Yahoo, Google etc. The consumer gets to use the software alone and enjoy the benefits. Cloud computing is broken down into three segments: "application" "storage" and "connectivity." Each segment serves a different purpose and offers different products for businesses and individuals around the world. In June 2011, a study conducted by V1 found that 91% of senior IT professionals actually don't know what cloud computing is and two-thirds of senior finance professionals are clear by the concept, highlighting the young nature of the technology. In Sept 2011, an Aberdeen Group study found that disciplined companies achieved on average an 68% increase in their IT expense because cloud computing and only a 10% reduction in data center power costs.

1.5 INTRODUCTION TO TRUST BASED MODELS

Recent technology development in the fields of wireless communication has facilitated the extensive distribution of wireless networks which are reliable, accurate, flexible, inexpensive and easy to deploy. In many Enterprise applications, environment monitoring and battlefield spying, the nodes are vulnerable to be attacked by passive eavesdropping and active intrusion. Among the above hostile attacks, passive eavesdropping helps adversaries intercept private information. Active intrusion makes it possible for

adversaries to delete information, insert false information or impersonate nodes, which destroy the usability, integrality, security certificate and non-reputation of Wireless Networks. Unfortunately, the available complicated encryption algorithms are unsuitable for providing Security because of the restricted capabilities of low bandwidth and processing power of smartphones. The smartphones cannot adopt security method based on traditional symmetric and asymmetric cryptographic methods.

Trust management based on the trust models and trust policies [13] are fundamental to identify malicious, selfish and compromised nodes which have been authenticated [12]. It has been widely studied in many network environments such as peer-to-peer networks, grid and pervasive computing and so on. However, in reality, Smartphones have limited resources and other special characters, which make trust management for smartphones more significant and challenging. Up to the present, research on the trust management mechanisms on cloud have mainly focused on nodes' trust evaluation[1] to enhance the security and robustness.

Although there are some existing approaches play good roles in improving security of other networks, trust management on cloud still remains a challenging field. In this paper, we propose an middleware where the Trust evaluation Model will run and uses algorithm by analyzing the trust Policies and granting access to smartphones based on the trust values calculated by the middleware.

Wireless sensor networks suggest potentially beneficial solutions for various applications. A major feature of these systems is that sensor nodes in networks assist each other by passing data, in-network process and control packets from one node to another. It is often termed an infrastructure-less, self-organized, or spontaneous network. Because wireless sensor networks pose some unique challenges, traditional security techniques cannot be applied directly to the sensor networks. First, each sensor node is limited in its memory, battery life, computation, and communication capabilities; Therefore, computation-intensive techniques like public-key cryptography are not expected to be used in wireless sensor networks. Second, they are susceptible to a variety of attacks, for example node capture, eavesdropping, denial of services, wormhole, and Sybil attack. A major purpose of the active attackers is to make the entire or partial networks impractical or make the networks under the control of them. If the attacker can obtain their own commodity sensor nodes and induce the networks' to accept them as legitimate nodes, it is hard to distinguish legitimate nodes from illegitimate ones just through the current network security policies. In addition, such a distinction is also beyond the ability of the conventional key management scheme because we cannot guarantee the secrecy of each node's private key

2. PROBLEM DEFINITION

2.1 Smartphones accessing the Web Services

With the increasing wireless bandwidth, CPU speed, memory capacity and disk storage, mobile devices are now beginning to be used increasingly often as platforms for accessing IT resources. Corporations allow their employees using mobile devices to access enterprise web applications to improve efficiency at a reduced cost. Figure 3 below presents the structure of currently used web services access control system [10]. It includes smartphones accessing the Enterprises Applications hosted on cloud..

The clients can be mobile devices, laptops or desktops. Normally mobile devices like smart phones, tablets, PDAs connect mobile networks or Wi-Fi; Laptops connect cloud through Wi-Fi or fixed cables; Desktops connect through fixed cables then forwards these HTTP requests to different web applications based on the request types. Web applications respond to these requests, retrieve information from databases and send them back to the clients.

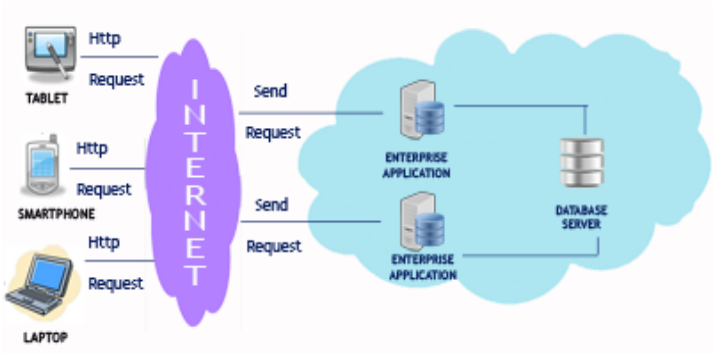

Fig 3: Different devices accessing Enterprises Application on Cloud.

When it comes to mobile devices' interactions[3] with the web services, there are challenges for security and trust among the devices. Mobile devices are typically small and portable devices which use no-fixed infrastructure, no central administration network to access enterprise web services. Figure 3 above shows the mobile clients accessing the enterprise applications deployed on cloud.

The convenient of access and vulnerability of network introduces more attacks. The potential risks for mobile devices in composite web services system are:

2.1.1 Lost or Stolen Devices: Smartphones because of the mobility tend to be less secured, since their users want fast access and prefer to avoid tedious login procedures due to the text interface constraints of mobile devices; and the mobile devices are usually small and carried to all kinds of place, so the chances for being used by other people or stolen are much higher than for a traditional desktop/laptop. Not only may some resource be leaked out to unauthorized users, but it also can be used as an attack tool for some fragile web services.

2.1.2 Insecure Communication: The communication channel between the Smartphones and Cloud has to be more secured as the wireless signals can be sniffed from anyone within the range of the network.

2.1.3 Abuse of Privileges: Even legitimate users can cause security issues due to their misbehavior. Since the mobile devices are carried everywhere all the time, the chance for abusing privileges is much higher than for desktops/laptops.

2.1.4 Traditional Access Control Issues: Composite web services, especially some cross-domain web services, contain multiple tasks. This leads to the question of how to aggregate multiple services into one logic unit safely. By using authentication access control, we assign users privileges for each domain and service. While assigning a user privilege for a certain task is relatively easy, it is complicated to assign privileges to a user for multiple tasks. Assigning a user privileges cross-domain can cause potential risks. Composite web services must keep changing to adopt to dynamic and

increasing business requirements, but current authorized web access may not be sufficient for future or have more than enough access privilege.

3. PROPOSED MIDDLEWARE TRUST MODEL ARCHITECTURE ON CLOUD

To resolve these risks mentioned above, I have proposed a Middleware to enhance security for Smartphones Accessing web services. As shown in figure 1-2 below, there are trust modules and trust policies for each web services. When mobile devices invoke web services, they send context information along with http requests. The trust modules handle the http requests before they are sent to web services and calculate trust and reputation of coming requests based on trust policies set by the corporation. If the trust value of the request is not higher than a certain value, it is rejected by the system. Thus, in addition to the traditional authentication access control[10], we enable trust/reputation mechanisms for enterprise web services.

3.1 Middleware for Cloud

Minimal overhead and robustness are required for the system as there are distributed trust models and trust policies for each web application [17].

Figure 4 below shows how the middleware is hosted on the cloud which acts as intermediate between the smartphones and the Enterprise Applications. The initiative of this Secure architecture is to offer the Middleware Architecture which is:

3.1.1 Adaptable and Flexible: This trust model should be flexible to accept the dynamic variable business processes and policies so that Trust policies can be adjusted efficiently [14].

3.1.2 Security: The Trust Models and Trust Policies in the Middleware will calculate a trust value of each customer and based on that trust value the access will be given to smartphones [18].

3.1..3 Scalability: Scalability becomes an important factor with the rapid growth of mobile devices and the massive variety of mobile services[8]. The system should be able to handle a large amount of concurrent requests without significant performance degradation.

3.1.4 Optimized Communication: Although the performance of hardware for mobile devices has appreciably enhanced, there is still a limit for wireless connection, computing capability and storage. Reducing the complicity of user interface and minimize the data flow are desired [6].
Whenever a smartphone is accessing the enterprise application on a cloud, there are different trust factors which control the trust in such a mobile environment. Trust in case of Smartphones is an assurance to an action based on a belief that the future actions of that smartphone will lead to a good result. This explanation forms the basis for identifying main factors that influence the trust in mobile systems, and how it can be used in computation. Our cloud based trust model has direct trust. When a peer has enough interacting experience with another smartphone of cloud, direct trust is the trust of a smartphone on another based on the direct interacting experience and is used to evaluate trustworthiness.

The cellular network environment is more distributed, with wider participants and more autonomic than the fixed network. Since there is no centralized node to serve as an authority to monitor and punish the peers that behave badly, malicious peers have an inducement to provide poor quality services for their benefit because they can get away. An important question raised is how can a mobile peer owner decide one or more peers to interact with it? In other words, what should be the selection criteria on which the mobile peer owner makes the interface decision? Obviously, the smartphone owner should select the services from other enterprise applications on cloud of other smartphones that have a satisfactory level of trust. In cloud based distributed trust model [7] , trust is measured by a trust value.

3.2 Trust value on Cloud

The trust value is the function of the following parameter.

3.2.1 Satisfaction or dissatisfaction degree in interactions:

When a mobile peer finishes an interaction with another peer, the mobile peer will evaluate its behavior in the interaction. The result of assessment is described using satisfaction or dissatisfaction degree which is in the range (-1, 1). Satisfaction and dissatisfaction degrees express how well and how poor this peer has performed in the interaction.

3.2.2 Number of interactions by Smartphones:

Some peers have A smartphone will be more familiar with other peers by increasing the number of interactions. A smartphone accessing the cloud more occasionally than other will have more trust developed than the smartphones accessing very rarely.

3.2.3 Size of Interactions:

The size of interaction expresses the file size shared in each interaction, while in a Web based business community, it shows the sums of money involved in each interaction.
Size of interactions is an important factor that should be considered in the trust model. If size it is set too low, it would make it more difficult for a peer to show trustworthiness through its actions. If it is set very high, there may be a need to limit the possibility for peers to start over" by re-registration after misbehaving.

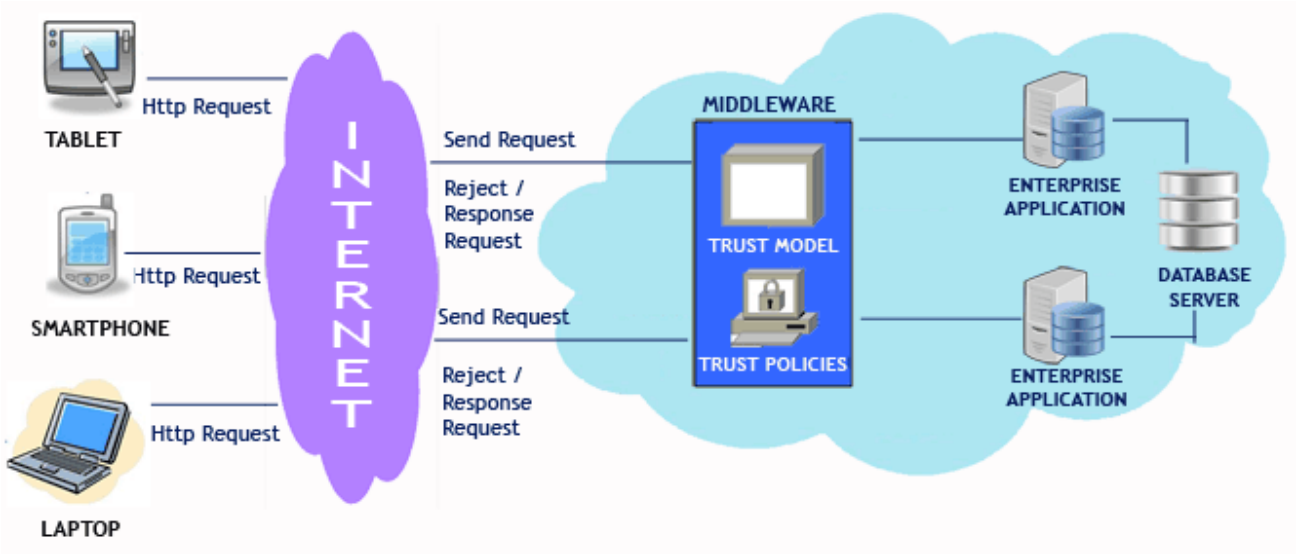

Figure 4: Middleware on Cloud which is enabling the secure communication between the smartphones and Enterprise Applications

In our trust model, the introduction of the size of interactions effectively solves the trust problem of peers without any interacting history

3.2.4 Interaction Time: The influence of an interacting history record to trust always decays with time. The more recent interactions have more influence on trust evaluation of a peer. For instance, if peer X has interacted with peer Y for a long time, the change of trust degree influenced by the interaction three years earlier is weaker than that of today. In our trust model [18], we introduce time factor to reflect this decay, that is, the most recent interaction usually has the biggest time factor.

3.2.5 Punishment function: The measurement of trust can be both positive and negative and the decay of Influence of the interaction experiences with time becomes less, and it also punishes malicious actions. Punishment should be involved by decreasing its trust degree according to the amount of malicious behaviors. The punishment factor the middleware model to be used to fight against subtle malicious attacks.

3.2.6 Risk Factor: Every peer has its own security defense ability which is reflected by risk factor, such as the ability to detect vulnerabilities, the ability to address any viruses and to defend against intrusions.

If Smartphone X wants to interact with Enterprise Application Y in order to accomplish a certain task.
Mobile X won't interact unless it is sure that Application Y is trustworthy. In order to find out whether Application Y is trustworthy, Mobile X will calculate a trust value for The Application Y.
When Mobile X has enough interaction experience with Y, X uses direct trust to calculate the trust value for Y. On the other hand, when Mobile X doesn't have enough interaction experience with Application Y, Mobile X uses recommendation trust to calculate the trust value for peer Y.

3.2.7 Cloud Trust Value: Direct trust is denoted as D(Tx (y),S). Where $Tx(y)_{Cloud}$ is the direct trust value that Smartphone X calculates for peer the Enterprise Application Y. S expresses Applicatio n Y's level of size of interaction which is granted by Smartphone X.

The Cloud Trust value $Tx(y)_{Cloud}$ is defined as:

$$T_x(y)=\alpha^* \sum_{i=0}^{N(y)} \left(\frac{S(x,y)*M(x,y)*Z}{N(y)} pun(i) \frac{1}{1+e^{-n}}\right) + \beta Risk(y) + \gamma Risk(Cloud) \quad \text{----------} \quad (1)$$

Where α , β and γ are weighting factors that satisfies the condition α +β=1 . N(y) is denoting the total number of interactions that Smartphone X has performed with Enterprise Application Y and S(x,y) denotes the Smartphone's X's satisfaction degree of interaction in its ith interaction with Enterprise Application Y which is in the range of (-1, 1). *M*(*x*,*y*) is the ratio between the size of the ith interaction and the average size of interactions which reflects the importance of the *ith* interaction among all the interactions that Smartphone X has performed with Enterprise Application Y.

Therefore $M(x,y) = \frac{m_i}{m_y}$, where m_i is the size of the ith ith interaction and *mv* is the average size of all interactions. We use Z to denote the time factor.

$$\mathbf{Z} = u(t_i, t_{now}) = \frac{1}{t_{now}-t_i} \quad \text{----------} \quad (2)$$

where t_i is the time when the ith interaction occurs and t_{now} is the current time. $\frac{1}{1+e^{-n}}$ is the acceleration factor where *n* denotes the number of failures. It can make trust value drop fast when an interaction fails. As this factor increases with *n* , it helps avoid heavy penalty simply because of a few unintentional cheats. Finally, *Risk*(*y*) is used to express the risk factor. *pun*(*i*)denotes the punishment function and

$pun(i)=\begin{cases}1, & i\ the\ ith\ interaction\ fails\\ 0, & if\ the\ ith\ interation\ succeeds\end{cases}$

Finally, the $\gamma Risk(Cloud)$ is used to add the risk factor due to the cloud vulnerabilities.

If the trust value T(y)x_{Cloud} calculated will be less than the threshold value then the smartphone users would be rejected as their satisfaction degree and trust value of less than the required value to be granted permission to access [2] the Enterprise Application on the cloud.

The entire middleware would be simulated on cloudsim and an android application will be made to access a web portal running on enterprise server on the cloud. The access would be granted after calculating the trust value of the smartphones accessing the application.

4. CONCLUSION

It is getting more and more common to access data either on Cloud or web servers by accessing the enterprise applications on the cloud by using smartphones. As the majority of the enterprise applications these days are on cloud and which is the future of hosting the enterprise applications their is need of a system where the security issues of the smartphones can be tackled properly for accessing the enterprise applications. The request performed by smartphones to access the enterprise applications are to be trusted for performing the communication but traditional methods of trusting the smartphones are not enough. The new trust models will enable is to calculate the trust value and allow the enterprise applications to be accessed by smartphones.

The Middleware on cloud will calculate and assess the trust value and reputation of smartphones The trust module on the Middleware is light weight component which can be attached to a distributed system on cloud. Every module works autonomously and also communicates with each other, exchanging trust information of smartphones and enterprise applications. The trust module calculates smartphones requests based on the different parameters like interactions and risks based on the trustworthiness of the domains. The main problems of lost or stolen devices, abuse of privileges and traditional access control issues can be controlled by the trust value of the devices. Normal mobile access control[11] and web access control[10] cannot solve these issues. By calculating the trust value based on mobile owners' operation patterns, mobile owners' normal working routine most of lost or stolen devices' cannot be used to access protected data.

The possibility of abusing the privileges is much higher in organizations which grant access to employees. With the limitation of sending location type and sending time, or other restrictions, abusing freedom can be reduced. The middleware trust module which is built on the top of the original security settings, calculates the requests from other domains based on the context values and trustworthiness of the other domains. It protects current domain from other malicious requests.

5. ACKNOWLEDGMENTS

My Sincere thanks to all my Professors for guiding me and choosing this topic for exploring latest technologies. I would like to thank the entire faculty for guiding me well.

6. REFERENCES

[1] A Distributed Trust Evaluation Model for Mobile, P2P Systems. Xu Wu, Department of Computer Science, *Xi'an University of Posts and Telecommunications*, Xi'an, China 2012.

[2] S. E. Abdrahman, "Web Access Control Using User Access Behavior (WACUAB)", Proceedings of the 2008, *International Conference on Semantic Web & Web Services (SWWS 2008)*, pages 242-5, 2008.

[3] Singh, M. and Dhindsa, K.S., 2013. "Enhancing Interaction between Smartphones and Web services on Cloud for improved Bandwidth and latency," *International Journal of Computer Science and Mobile Computing (IJCSMC)*, Vol. 2, No. 4, pp. 177-185.

[4] Y. Sun, W. Yu, Z. Han, and K. Liu, "Information theoretic framework of trust modeling and evaluation for ad hoc networks*," IEEE Journal on Selected Areas in Communication*, vol. 24, pp. 305–317, Feb. 2006.

[5] K. Takeshita, M. Sasabe, H. Nakano, "Mobile P2PVNetworks for Highly Dynamic Environments", in Proc. Of the 6th *IEEE International Conference on Pervasive VComputing and Communications*, Hong Kong, 2008, pp. 453-457.

[6] Singh, M. and Dhindsa, K.S., 2013."Securing RJSON data between Middleware and SMARTPHONES through JavaScript based Cryptographic Algorithms."*International Journal of Soft Computing and Engineering (IJSCE)*, Vol. 3, No. 2 , pp. 189-194..

[7] M. Singh and V. K. Prasanna, "A hierarchical model for distributed collaborative computation in wireless sensor networks," in Proc. of the17th *International Symposium on Parallel and Distributed Processing. Washington*, DC, USA: IEEE Computer Society, 2003, p. 166.2.

[8] R. Zhou and K. Hwang, "PowerTrust: A Robust and Scalable Reputation System for Trusted P2P Computing," *IEEE Transactions on Parallel and Distributed Systems*, Vol.18, No.5, May 2007.

[9] F. Alshahwan and K. Moessner, "Providing SOAP web services and RESTful web services from Mobile hosts", IEEE fifth international conference on internet and web applications and services, 2010.

[10] M. Coetzee and J. H. P. Eloff, "A Trust and Context Aware Access Control Model for web service conversation", Trust, Privacy and Security in Digital Business.Proceedings *4th International Conference, TrustBus 2007*. (Lecture Notes in Computer Science vol. 4657), pages 115-24, 2007.

[11] L. Bauer, M. A. Schneider, and E. W. Felten, "A Proof-Carrying Authorization System", *Proceedings DARPA Information Survivability Conference and Exposition*, 117-19 vol.2, 2003; ISBN-10: 0 7695 1897 4; DOI: 10.1109/DISCEX.2003.1194942; Conference: Proceedings DARPA Information Survivability Conference and Exposition, 22-24 April 2003.

[12] A. Corradi, R. Montanari, D. Tibaldi, A. Toninelli, and U. Bologna, "A Context-centric Security Middleware for Service Provisioning in Pervasive Computing," Symposium *A Quarterly Journal In Modern Foreign Literatures*, 2005.

[13] R. A. Shaikh, H. Jameel, B. J. d'Auriol, H. Lee, and S. L. and Young Jae Song, "Group-based trust anagement scheme for clustered wireless sensor networks," IEEE *Trans. Parallel and Distrib*. Sys, vol. 20, pp. 1698–1712, 2009.

[14] Forman, G. 2003. An extensive empirical study of feature selection metrics for text classification. J. Mach. Learn. Res. 3 (Mar. 2003), 1289-1305.

[15] Brown, L. D., Hua, H., and Gao, C. 2003. A widget framework for augmented interaction in SCAPE.

[16] Spector, A. Z. 1989. Achieving application requirements. In Distributed Systems, S. Mullender.

[17] M. Coetzee and J. H. P. Eloff, "A Trust and Context Aware Access Control Model for web service conversation", Trust, Privacy and Security in Digital Business. *Proceedings 4th International Conference, TrustBus 2007*. (Lecture Notes in Computer Science vol. 4657), pages 115-24, 2007.

[18] L. Eschenauer, V. D. Gligor, and J. Baras, "On trust establishment in mobile ad-hoc networks", In B. Christianson, B. Crispo, J. A. Malcolm, and M. Roe, editors, 10th *International Security Protocols Workshop, Cambridge*, UK, April 2002, volume 2845 of Lecture Notes in Computer Science, pages 47-66.Springer-Verlag, 2004.