Research Journal of Information Technology

ISSN 1815-7432

Academic
Journals Inc.

www.academicjournals.com

OPEN ACCESS Research Journal of Information Technology

ISSN 1815-7432
DOI: 10.3923/rjit.2016.47.54

Research Article
Self-Protection and Security in Mobile Cloud Computing

Mohammed S. Zahrani

Department of Computer Science, College of Computer Science and Information Technology, King Faisal University, Al-Ahsa, Saudi Arabia

Abstract

Mobile Cloud Computing (MCC) is an application of cloud computing. In MCC, all the data and applications previously embedded in mobile phones are made available on the cloud everywhere in the world. Besides, it makes the mobile phone storage space available. It enables the users to access the cloud while moving among different networks (foreign networks) and use different applications. So, the biggest risk factor is the security of this mobile cloud. This study represents a self-protection mechanism i.e., the property of autonomic computing was proposed to make the mobile cloud self protected without human intervention from intrusions and attacks. The architecture of self-protection of mobile cloud was presented and describes the basic interaction and functionality of each component of architecture.

Key words: Securing mobile cloud, mobile networks, cloud protection, wireless communication, data security

Received: January 20, 2016 Accepted: February 20, 2016 Published: March 15, 2016

Citation: Mohammed S. Zahrani, 2016. Self-protection and security in mobile cloud computing. Res. J. Inform. Technol., 8: 47-54.

Corresponding Author: Mohammed S. Zahrani, Department of Compute Science, College of Computer Science and Information Technology, King Faisal University, Al-Ahsa, Saudi Arabia Tel: 00966-504648188

Competing Interest: The authors have declared that no competing interest exists.

Data Availability: All relevant data are within the paper and its supporting information files.

INTRODUCTION

Cloud computing aims at making services and resources available on virtual platform i.e., cloud for users. The users can access all information and services without information about the hosting environment and its method of delivery (Fig. 1) according to Hashmi and Kumar (2013) and Perez (2010). The components of cloud computing includes client, service, application, platform, storage, infrastructure (Logan, 2012). The clusters of web servers provide the applications in the browsers for users. These web servers run user's interface softwares receiving the user's commands such as mouse clicks, key presses and uploads, etc. for their interpretation. As such, this process enables the users to store data on servers or can retrieve updated page from the database. Researchers have pointed out that multiple servers synchronize the data for global (Perez, 2010; Logan, 2012; Fabian *et al*., 2015).

The wireless cloud computing refers to the wireless usage of cloud computing i.e., accessing the cloud wirelessly. Whereas, Multiple Component Computing (MCC) focuses mainly on the use of cloud networks and its integration with mobile handheld devices (Fecht, 2012).

The MCC is a new and the latest computing era where all mobile devices exploit the available platform of cloud to perform distributed processing on multiple servers and access data remotely from different machines rather than using its own storage space (Fig. 1).

Generally, a mobile station sends the request to BTS for accessing the cloud. Then the BTS forwards the request to BSC and the related BSC will send the request to MSC. The MSC forwards the request to GMSC. Lastly, the GMSC allows the mobile station to connect to the cloud via internet platform which is available on virtual platform. Therefore, the mobile applications and the other related data are made available on this cloud for its users. At the backend of cloud, the servers along with the databases are made available as shown in Fig. 2.

The IBM introduced autonomic computing in 2001 (Fig. 3) which is currently an emerging research trend in software engineering due to its natural biological and human medical systems in order to minimize human intervention (Xiao and Xiao, 2013). The characteristics of autonomic computing contain self-intelligence attributes with the main goal to achieve self-management of data systems and its applications to the training level guidance from human beings (Parashar and Hariri, 2004). The self-intelligent attributes include self-configuration, self-healing, self-protection, self-optimization and self-awareness (Fleener *et al*., 2014).

Fig. 1: Mobile cloud computing

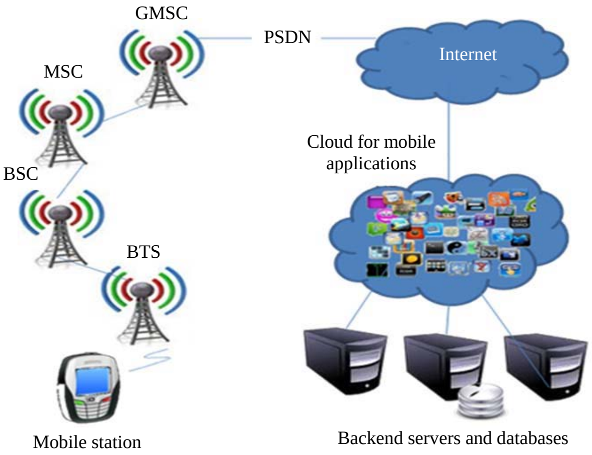

Fig. 2: Mobile Cloud Computing (MCC) architecture

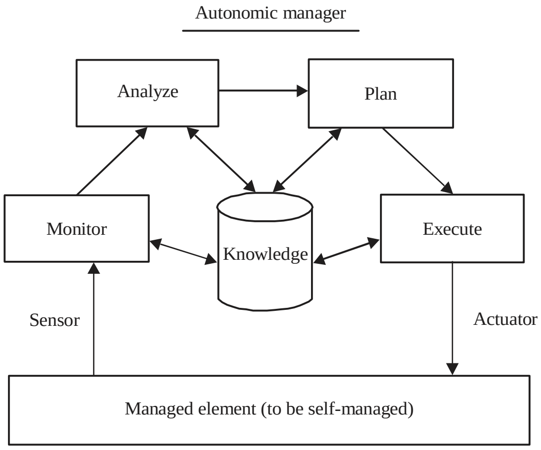

Fig. 3: Architecture of autonomic computing (Xiao and Xiao, 2013)

The self-protection mechanism is one of the intelligent attributes of autonomic computing which defines system's self-defense mechanism against an attack from attackers/hackers (Palmer, 2015). According to Jarrett and Seviora (2006), the self protection system is able to detect attack, performs a recovery and retrieval of any loss occurred due to attack. It is also a motivation from the protection mechanism of human body from viruses and diseases. The self-protection is the capability of the system to proactively defend and detect attacks and respond to them in real-time to protect its resources. Various types of attacks against which a system self-protects are Viruses, Intrusions, Denial Of Services (DOS) and Distributed Denial Of Services (DDOS). The DOS/DDOS attacks are performed to make the server down for a particular duration to make it unavailable and unable to provide services to its clients.

Presently, use of mobile is increasing day by day and data protection and security of the users is an important issue from privacy view point. Therefore, the main objective of this study was to propose a self protection methodology in a mobile cloud to protect it from attacks.

Currently, the mobile phones are reaching to users of all ages who started to utilize advanced capabilities of cell phones due to new applications. But the new applications need robust computing power handsets which limits them (Patidar *et al*., 2012). On the other hand, the mobile application developers are encountering the challenges of multiple mobile operating systems. Therefore, either the applications are to be written for a particular OS or the applications are provided with multiple versions. Moreover, applications require more processing power and memory in the mobile sets (Patidar *et al*., 2012).

Previously, most of the applications and websites were designed for desktop workstations. As such, it was difficult to view these websites and applications on small handy devices due to less memory, low computing power and small screens. Therefore, a new approach was adopted by different vendors to upgrade the communication services. This approach introduced two new components of the system i.e., distributed web page adaption engine and block management. The next most attractive expected application area includes games and mobile banking. Also the cloud lets people allow to remotely turn lights on or off, view recorded TV programs and use many services based on their saved profiles on cloud which helps them to save time and ease the process (Wang *et al*., 2013).

Smartcard web server is a technology mentioned by the Application Binary Interface (ABI) in which the Subscriber Identity Module (SIM) provides security mechanism by direct integration with the applications from different public network to cellular phones. There are other applications such as 'Toktok' which helps the users to automate the process of search as mobile applications directly communicate with the service without navigating the browser of the mobile (Sterritt *et al*., 2005; Perez, 2010).

There are many new applications in medical industry being introduced based on cloud computing to facilitate patients remotely to make the health technology systems cost effective and affordable to all the patients with quality of service. The results from inexpensive low end Ultrasonic transducer designed for 2D at a remote location of patient can be converted into high end 3D UV scanners with more centralized computing power using cloud infrastructure (Wang *et al*., 2013). As mentioned in Fig. 4, a network cloud provides all the operational services such as, computational resources for those operating in a cloud platform. The I/O throughput, virtual Base Stations (BS), timing networks for synchronization etc., were the challenges involved in computational power requirements of several complex systems (Lin *et al*., 2010). Vendors such as Microsoft, Amazon, Google etc. (the real time examples of cloud computing) provides secure cloud platform that includes cloud management, cloud applications, cloud engine and cloud servers (Ashalatha, 2012).

Autonomic Computing (AC) and its features enable the development of different systems and applications using its self-attribute namely the self-management, using autonomic strategies, procedures and its sensitive algorithms to solve complex problems automatically with less interventions of human. Autonomic elements such as intelligent control loops for monitoring purposes, sensing of knowledge environment which helps in planning, analyzing and execution are the main blocks of this computing system (Parashar and Hariri, 2004).

A thorough study of Fig. 4 shows its autonomic nature based on self-management of its components. Autonomic computing is flexible in nature as its design is acceptable in most of the domains with minor modifications of current system (Fua and Oudshoorn, 2007). Autonomic computing is a step towards pervasive computing of future era where small handheld devices will be communicating with each other through larger networks probably the cloud networks. The IT systems and security issues can be fixed automatically without human intervention or less guidance. Because, it has better uptime and reduced IT costs due to its less human resource requirement to manage due to its self-management attributes (Zhou *et al*., 2011).

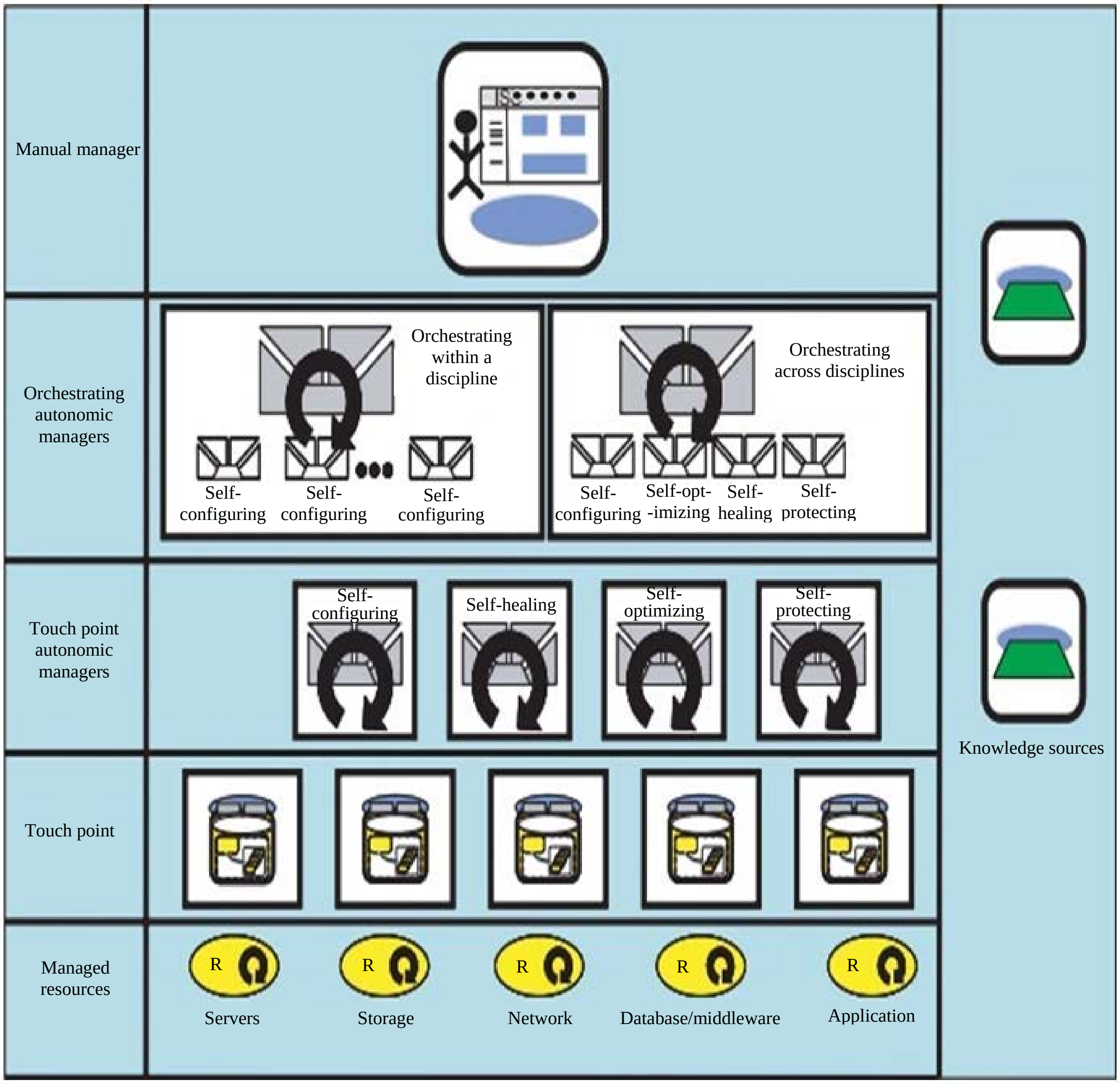

Fig. 4: Autonomic computing architecture by IBM Parashar and Hariri (2004)

The threats to mobile cloud security are increasing day by day due to its increased commercial popularity (Zhang *et al*., 2010). The corporations and governments are moving to cloud based models by accessing devices from anywhere for application as a regular practice. There is a huge trend of transition towards cloud platform in private industry as well. It replaces carrying big machines with tablets and smart phones. Cloud service providing companies are figuring out this trend and supporting various handheld devices and its platforms like Android and IOS. However, continuous trend of population towards these mobile devices makes this service more attractive and lucrative (Jarrett and Seviora, 2006; Zhou *et al*., 2010).

Information security is also undergoing a transformation as moving to a cloud service model. Some basic views such as defense in depth and principle of least privilege, are still in trend, but security systems such as, Intrusion Detection Systems (IDS), perimeter security and other broad based defenses becomes less and less important as the focus is turned to more atomic protection. Current information security systems are focusing on the authentication, identification and protection of data itself instead of physical environments such as, network and SAN devices, servers, etc. where the actual data resides in and move (Ziqing, 2010).

To overcome the data loss and availability problem, data in the cloud is replicated and stored in different locations that is unknown to the customers. Data may be stored in different places or in different country. Here, the security concern here is that data secured in one country may or may not be secured in other due to different laws. For example, data stored in

Europe comes under EU legislation and in US comes under US legislation which are different from each other (Bhavani and Hatwal, 2015). Mutual protection in cloud computing architecture was also proposed at a research level in order to discuss the mutual trust and the definable profiles of communicating systems. The objective of the proposed architecture was to achieve better and flexible security and authentication based on the concept of mutuality of trusted profiles within the cloud computing environment (Albeshri and Caelli, 2010).

A mobile cloud framework called Mobicloud provides traditional cloud computation services. However, issues such as risk management, secure routing and trust management are handled by MobiCloud thus enhancing its communication ability. Besides, new applications can be built on the MobiCloud framework which can increase the processing power of small devices to act efficiently in cloud environment (Huang *et al*., 2010, 2011).

An Autonomic Security Policy Framework (ASPF) was introduced as a policy based security framework for self-protection of distributed networks. It ensures that all the security and authentication policies on small handheld devices are configured and adapted according to the authentication parameters compliant with cloud services. It also explores the autonomic security of the cloud system which may control Operating system level authorization schemes and also supports multiple classes of its policies (He *et al*., 2010; Tsai and Lin, 2011). Robust security models for cloud computing are in demand for securing cloud based infrastructure development and its deployment in the real world. The objective of the model was to exploit the Service Oriented Architecture (SOA) safely. It also needs to secure its infrastructure, associated services, cloud service provider's data and all hardware devices linked with users and providers which are shared on SOA. The SOA provides a wide variety of secured flexible features which can be used in the system to fix the vulnerabilities and secure all linked systems and services (Shahbazi *et al*., 2013; Ahmed and Hossain, 2014).

As with any security program, the requirements are a starting point and baseline to be tailored in a given system. For cloud service providers and system owners, a clear and upfront delineation of security control responsibilities seems more important than ever (Fleener *et al*., 2014). The technical mechanisms for accountability in cloud computing include encryption and decryption methods for data security and privacy. Moreover, accountability can provide transparency between CSP and customers if they trust each other and CSP achieve their obligations towards their customers. Cloud Platforms Social Networks (CPSN) are scalable cloud applications hosted by profitable clouds such as, Facebook (FB). The applications of FB are hosted by Amazon Web Service (AWS) platform and the design architecture for FB application in social cloud computing network is typically similar to PAAS architecture (Buyya *et al*., 2010). Application programming Interface (API) of FB provides a set of information about users such as the friends list, groups, application users, events, photos and profile information (Al-Tehmazi and Al-Jobori, 2015).

Presently use of mobile service in increasing due to its easy access and handling. However, the protection and security of user's data in vulnerable to various types of attacks. Therefore, the main objective of this study was to propose a model which is more reliable for self protection and security of mobile cloud computing.

MATERIALS AND METHODS

For securing mobile cloud, self protection scheme based on the concepts of autonomic computing was applied to mobile cloud (Jarrett and Seviora, 2006). The backend, where data and applications are residing in databases and servers, requires high security. They require the protection against attacks such as malware, viruses, DDOS, DOS and intrusions. The attacks can result into disruption of the functionality of cloud. Here the architecture of self protection of a cloud was proposed as outlined in Fig. 3. The architecture comprises managed element and autonomic manager. The managed element is a mobile cloud along with the backend entities. The autonomic manager continuously keep on monitoring the cloud for attacks or any intrusions towards the cloud. If it senses any intrusion, then it forwards the case for monitoring. Then analyze it, suggests optimal plan using the knowledge with a solution for final application to the managed element.

RESULTS AND DISCUSSION

The proposed model is presented in Fig. 5. The knowledge in the autonomic manager is its database related to information of viruses, intrusions, various types of attacks and their properties. The model also includes the remedies to these attacks. Whenever any attack is sensed, the case is under observation in the monitor element. The knowledge base is then consulted. The knowledge base includes a large database and uses signature based systems to detect attacks by cross-referencing the attack signature from its database. As the cloud data comes from some heterogeneous data sources over multiple networks, then the knowledge base detects various attacks by matching its signature. Also, it has the

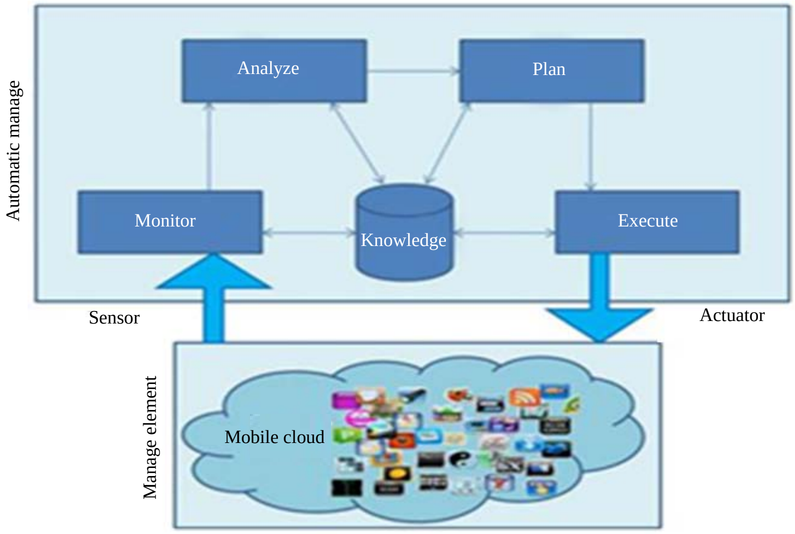

Fig. 5: Architecture of self protection of mobile cloud computing

ability to look for strings in authentication process which might indicate an attack in progress and detect the malicious bits that are passed through during the time of attack by comparing its database. The basic requirement of the proposed architecture of self-protection of mobile cloud computing is to keep the knowledge base update and it should be semantically richer to combat any known attack on our cloud network.

The analyze component analyzes the case by searching for the matching cases to the one encountered in the knowledge base. Whereas, it performs a statistical analysis to look for deviations from the normal behavior of data and detects any anomaly in the state of the applied cloud security system. It also includes, a policy language for translating service provider's policies into analysis rule set.

A plan to suggest the remedy is done by plan. The nearest matching cases are taken into consideration, then the results are used as a solution for the encountered attack. If the solution of the nearest cases does not fulfill the demand then a merged solution is proposed for execution. If it is successful in its attempt then the case is retained in knowledge base along with its solution. Finally, the plan component is ought to generate a plan based on the significance of attack level. Besides, if the attack level is high, it will immediately send a response to managed element to block the attack. Above all, it can also lock the attacker to get evidence for legal prosecution but not at the cost of compromising user's data on cloud.

The study results agree with the findings of many investigators who reported that self protection of mobile cloud computing need to deploy various distinct technologies such as, intrusion detection systems, firewalls, integrity monitoring, malware protection and log inspections as a software on virtual machines to enhance the security and protection of the servers due to the mobility of virtual resources on these servers from different heterogeneous networks to public cloud environments (Qaisar and Khawaja, 2012; Sharma *et al*., 2012; Ashktorab and Taghizadeh, 2012; Chuang *et al*., 2011; Dinh *et al*., 2013).

CONCLUSION

Securing cloud from the attacks and attackers is a need of today. Compromising a cloud can result into information loss or unethical access to unauthorized users. Therefore, this paper presented a protection strategy to keep the cloud protected from intruders or unauthorized users. Moreover, the cloud contains an autonomic element of self protection for monitoring and protecting the cloud itself without human intervention. The proposed strategy can be tested and experimented to collect the accuracy of approach. Depending upon the results further improvements can be made to it.

REFERENCES

Ahmed, M. and M.A. Hossain, 2014. Cloud computing and security issues in the cloud. Int. J. Network Secur. Applic., 6: 25-36.

Al-Tehmazi, D. and H. Al-Jobori, 2015. Trust relationship model to enhance security and privacy for cloud environment. Proceeding of the 3rd International Conference Advances in Computing Communication and Information Technology, January 2015, India, pp: 111-117.

Albeshri, A. and W. Caelli, 2010. Mutual protection in a cloud computing environment. Proceedings of the 12th IEEE International Conference on High Performance Computing and Communications, September 1-3, 2010, Melbourne, VIC., pp: 641-646.

Ashalatha, R., 2012. A survey on security as challenges in cloud computing. Int. J. Adv. Technol. Eng. Res., 2: 1-4.

Ashktorab, V. and S.R. Taghizadeh, 2012. Security threats and countermeasures in cloud computing. Int. J. Applic. Innov. Eng. Manage., 1: 234-245.

Bhavani, S. and A. Hatwal, 2015. Review on cloud computing and security issues in cloud. Int. J. Adv. Eng. Res. Sci., 2: 21-24.

Buyya, R., J. Broberg and A.M. Goscinski, 2010. Cloud Computing: Principles and Paradigms. Vol. 87, John Wiley and Sons, New York, ISBN: 9781118002209, Pages: 664.

Chuang, I.H., S.H., Li, K.C. Huang and Y.H. Kuo, 2011. An effective privacy protection scheme for cloud computing. Proceedings of the 13th International Conference on Advanced Communication Technology, February 13-16, 2011, Seoul, pp: 260-265.

Dinh, H.T., C. Lee, D. Niyato and P. Wang, 2013. A survey of mobile cloud computing: Architecture, applications and approaches. Wireless Commun. Mobile Comput., 13: 1587-1611.

Fabian, B., A. Baumann and J. Lackner, 2015. Topological analysis of cloud service connectivity. Comput. Ind. Eng., 88: 151-165.

Fecht, C., 2012. When did cloud computing come into existence? http://www.answers.com/Q/When_did_cloud_computing_come_into_existence.

Fleener, G., C. Zou and J. Eddy, 2014. Cybersecurity impacts of a cloud computing architecture in live training. Proceedings of the Interservice/Industry Training, Simulation and Education Conference, December 2014, Orlando, FL., pp: 1-11.

Fua, M.M. and M.J. Oudshoorn, 2007. System architecture of an autonomic element. Proceedings of the 7th IEEE International Conference and Workshops on Engineering of Autonomic and Autonomous Systems, March 26, 2007, Tucson, AZ., USA., pp: 89-93.

Hashmi, Z. and V. Kumar, 2013. Cloud computing. http://www.authorstream.com/Presentation/aSGuest16129-171391-cloud-computing-ppt-bmitians-education-powerpoint/.

He, R., M. Lacoste and J. Leneutre, 2010. A policy management framework for self-protection of pervasive systems. Proceedings of the 6th International Conference on Autonomic and Autonomous Systems, March 7-13, 2010, Cancun, pp: 104-109.

Huang, D., X. Zhang, M. Kang and J. Luo, 2010. MobiCloud: Building secure cloud framework for mobile computing and communication. Proceedings of the 5th IEEE International Symposium on Service Oriented System Engineering, June 4-5, 2010, Nanjing, pp: 27-34.

Huang, D., Z. Zhou, L. Xu, T. Xing and Y. Zhong, 2011. Secure data processing framework for mobile cloud computing. Proceedings of the IEEE Conference on Computer Communications Workshops, April 10-15, 2011, Shanghai, pp: 614-618.

Jarrett, M. and R. Seviora, 2006. Diversity to enhance autonomic computing self-protection. Proceedings of the 1st International Conference on Availability, Reliability and Security, April 20-22, 2006, Canada, pp: 295-299.

Lin, Y., L. Shao, Z. Zhu, Q. Wang and R.K. Sabhikhi, 2010. Wireless network cloud: Architecture and system requirements. IBM J. Res. Dev., Vol. 54. 10.1147/JRD.2009.2037680

Logan, A., 2012. What is a cloud computing? http://www.answers.com/Q/What_is_a_cloud_computing.

Palmer, K.D., 2015. Autonomic computing and special systems theory. https://www.researchgate.net/publication/265042962.

Parashar, M. and S. Hariri, 2004. Autonomic computing: An overview. Proceedings of the International Conference on Unconventional Programming Paradigms, September 15-17, 2004, France, pp: 257-269.

Patidar, K., R. Gupta, G. Singh, M. Jain and P. Shrivastava, 2012. Integrating the trusted computing platform into the security of cloud computing system. Int. J. Adv. Res. Comput. Sci. Soft. Eng., 2: 1-5.

Perez, S., 2010. Mobile cloud computing: $9.5 billion by 2014. http://readwrite.com/2010/02/23/mobile_cloud_computing_95_billion_by_2014.

Qaisar, S. and K.F. Khawaja, 2012. Cloud computing: Network/security threats and countermeasures. Interdisciplin. J. Contemp. Res. Bus., 3: 1323-1329.

Shahbazi, A., J. Brinkley, A. Karahroudy and N. Tabrizi, 2013. A distributed key based security framework for private clouds. Int. J. Adv. Comput. Sci. Applic., 4: 79-83.

Sharma, M., H. Bansal and A.K. Sharma, 2012. Cloud computing: Different approach and security challenge. Int. J. Soft Comput. Eng., 2: 421-424.

Sterritt, R., M. Parashar, H. Tianfield and R. Unland, 2005. A concise introduction to autonomic computing. Adv. Eng. Inform., 19: 181-187.

Tsai, C.L. and U.C. Lin, 2011. Information security of cloud computing for enterprises. Adv. Inform. Sci. Service Sci., 3: 132-142.

Wang, C., S.S.M. Chow, Q. Wang, K. Ren and W. Lou, 2013. Privacy-preserving public auditing for secure cloud storage. IEEE Trans. Comput., 62: 362-375.

Xiao, Z. and Y. Xiao, 2013. Security and privacy in cloud computing. IEEE Commun. Surv. Tutorials, 15: 843-859.

Zhang, X., S. Jeong, A. Kunjithapatham and S. Gibbs, 2010. Towards an Elastic Application Model for Augmenting Computing Capabilities of Mobile Platforms. In: Mobile Wireless Middleware, Operating Systems and Applications, Cai, Y., T. Magedanz, M. Li, J. Xia and C. Giannelli (Eds.). Springer, New York, ISBN: 9783642177583, pp: 161-174.

Zhou, M., Y. Mu, W. Susilo, M.H. Au and J. Yan, 2011. Privacy-preserved access control for cloud computing. Proceedings of the IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications, November 16-18, 2011, Changsha, pp: 83-90.

Zhou, Y., Y. Yang, L. Liang, D. He and Z. Sun, 2010. An agent-based scheme for supporting service and resource management in wireless cloud. Proceedings of the 9th International Conference on Grid and Cooperative Computing, November 1-5, 2010, Nanjing, pp: 34-39.

Ziqing, J., 2010. Security technology of the mobile internet cloud computing platform. Comput. Applic. Technol., 30: 72-74.