IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-7, Issue-2, Feb 2019 E-ISSN: 2347-2693

Revisiting Cloud Security Threats: Man-in-the-Middle Attack

Vaishali Singh[1*], Kavita Bhatia[2], S. K. Pandey [3]

[1]Dept. of CS, St. Xavier's College, Jaipur & Jagannath University, Jaipur,
[2,3]Govt. of India, Ministry of Electronics & Information Technology, New Delhi, India

**Corresponding Author: vaishalisingh@stxaviersjaipur.org*

DOI: https://doi.org/10.26438/ijcse/v7i2.342348 | Available online at: www.ijcseonline.org

Accepted: 12/Feb/2019, Published: 28/Feb/2019

***Abstract*—**Cloud Technology is an emerging technology that has improved the performance of many organizations by utilizing minimum resources and maximum outcomes. Cloud provides virtualized services, applications and can store a large amount of data from various locations. As the cloud environment is accessed through Internet, it cannot be trusted blindly. Thus security is considered as major barrier for users to adopt Cloud, where threats are considered as the major reason for the degradation of the quality of services. For effective use of cloud services, individual focus on the cloud threats is required and an approach is needed from the end user side to gain knowledge about various threats pertaining inside a cloud infrastructure. In the cloud deployment process, various network protocols are used to establish the connectivity between the infrastructure, services and clients. As a result, the server-end needs to be enough strong to provide security to network transmission. However, still the invader secretly accesses the transaction and modifies the communication between two parties. This invader gives birth to most common and critical Man-in-the-Middle (MiTM) attack. The aim of the paper is to re-examine 'Man-in-the-Middle' attack and its root causes. The focus is to present a broad indication on 'Man-in-the-Middle' attack, rising as an imperative security concern in cloud computing. The research study aims to review the previous literature and to emphasis on conclusive findings for future research in the related domain based on the published work and industry/organization reports.

***Keywords*—**Cloud Computing, Cloud Security, Cloud Threats, Man-in-the-Middle Attack, MiTM

I. INTRODUCTION

Cloud computing is a set of services and resources offered by a company over the internet and based on 'Pay as you use' [1]. In the cloud, data is stored in different premises. Cloud is used as a metaphor, as the Internet, which has a basic formation like clouds in the sky [1]. It does not have any fixed structure, and moves randomly. Cloud network enables resources movement at the remote endpoints for accessing the services and application.

However, due to advance benefits, the complexity of the cloud environment increases and networking becomes more complicated as compared to traditional networking [1]. Multiple cloud providers share resources between different networks across private, public and hybrid clouds [1]. With this, cloud offers the benefits of flexibility and scalability but without enough security, these benefits increase the risks and vulnerabilities in services.

Security is a major issue with increasing in the advancement of cloud computing and enhancing risk of data been stolen or manipulated by someone [2]. Still, cloud environment experiences the same threats that are in the traditional network system. Cloud computing processes run on various online software having loopholes through which the invader tries to take advantage of vulnerabilities [3]. Some common threats of cloud computing are data loss, data breach, denial of service, cloud abuse, network threats, luring threat, repudiation, replay attack, elevation of privilege attack and malware attack etc.[3]

One of the most common attack, where the malicious attackers redirect the legitimate user towards a fake site [4]. This type of mechanism is known as eavesdropping and the intruder is the Man-in-the-Middle attacker, who sets up the connection between the users for the false communication and fake information [4]. There are different ways to detect and prevent the MiTM attack like Cain, Dsniff, Airjack and Wsniffetc [5].

For efficient utilization of cloud secured services, we need to provide emphasis on Man-in-the Middle-attack individually. Further than the introduction of cloud, rest of this paper is well thought-out as follows. Section II provides the *overview of Man-in-the-Middle attack* with a detailed description based on *root cause study*. Section III highlights the *Survey on Related Works* and section IV depicts the "*Conclusive Finding"* based on the prior study. Finally, "*Conclusion and Future work*" in the section V.

II. ROOT CAUSE STUDY

Man-in-the-Middle attack occurs when attacker get an illegal access to confidential information [6]. It happens generally when two parties are communicating and the third party eavesdrop their private conversation [7]. In this process two original parties appear to communicate normally as they do not know that a third person is trying to access their private information [7]. Man-in-the-Middle attack mostly occurs on wireless network [8].

Generally, invader tries to discover unsecure Wi-Fi and eavesdrop the personal information [8].There is a need to find main root cause of the threat for finding the mitigation technique. Major facts for occurrence of Man-in-the-Middle attack are given as under:

(i). ***Absence of awareness about the security issues in networking [9]:*** As the attackers are very smart, they secretly relay on the communication, they know that the end users will directly communicate without the security with each other according to him and then will alter the information.

(ii). ***Name collision issue [10]:*** After launching the standard browser, name collision issue automatically redirect the Internet WEB traffic towards the Man-in-the-Middle proxy.

(iii). ***Internal leakage of Web Proxy Auto-Discovery (WPAD) protocol [10]:*** It is less studied issue and was not easy to exploit prior to the current original generic Top-Level Domains allocation.

(iv). ***Weak control on real-time processing of transactions [11]:*** The MiTM is just like session hijacking. Thus vulnerabilities like cookies information in unencrypted form of logins, and are stolen through sniffing the cookies data packets.

(v). ***Dishonest principles based Wi-Fi networks [12]:*** Users are less knowledgeable about the illegitimate networks. This is the loophole where an attacker easily launches the MiTM between network and user without trust.

(vi). ***Sniffing Issue [13]:*** The malicious attacker uses eagerly accessible software to intercept facts being sent between user and network

(vii). ***Improper configuration of authentication mechanism***: [14] Sender needs to apply encryption technique properly and simultaneously the receiver needs to have a proper security by applying decryption technique.

(viii). ***Improper configuration of Secure Socket Layer [15]:*** Attackers easily interpret and access the data transmitted between the two end users due to improper configuration of SSL. It is common in cloud where data communication is maliciously accessed without permission from the data centre due to the weaknesses in SSL configuration

(ix). ***Distribution of free malware on web browser [6]:*** The common methods for executing the Man-in-the-Middle attack are through distribution of malicious assets on web browsers of users. The malicious user easily controls the transactions and conversations from where they redirect their malicious activity to the user. They creates proxy sites for reading, modifying and for inserting the traffic between the justifiable sites and users.

(x). ***Forged certificates [16]:*** The endpoint authentication uses the cryptographic protocols that provide the trusted certified authorization to both parties mutually. However, before the user observes the malicious certification warning, the Man-in-the-Middle completes the execution attack.

(xi). ***Vulnerabilities in wireless router's configuration [17]:*** One of the issue through which the Man-in-the-Middle attacker takes the advantage is the improper security configuration of wireless routers due to weak passwords management.

(xii). ***A variety of protocols threats prop up Man-in-the-Middle attack [18]***: The attackers uses different other ways to indulge the Man-in-the-Middle attack with other attacks like Internet Control Message Protocol (ICMP) redirection, port stealing, traffic tunnelling and route mangling etc.

(xiii). ***No restriction for sensitive sites [19]***: No restrictions are established for prohibiting the logins for sensitive sites by the public networks, which are not registered**.**

III. SURVEY ON RELATED WORKS

The purpose of this section is to mostly re-consider the prior literature covering a variety of aspects of Man-in-the-Middle attack and to provide conclusive findings in order to facilitate future research study on the threats and their mitigation techniques.

The survey criteria has tried to majorly inculcated the overviews, vulnerabilities risks and active mitigating measures related to Man in the middle attack in cloud computing from various published work in articles, reports, and research paper. Major contributions in the related area are given as under:

(i). ***Man in the cloud attack [20]*****:** In the current study the Man-in-the-Middle attack is not considered as a new attack and is very well exploited. Man in cloud does not require any malicious code to get in command instead they rely on some type of common file synchronization service. To overcome this difficulty adaptation of some explicit files and registry key can be done.

(ii). ***What is a Man-in-the-Middle Attack and How Can You Prevent It? [6]:*** MITM attack can take place in any outline of online communiqué where two

systems is intercepted by an external party. Email Hijacking, Session Hijacking and Wi-Fi Eavesdropping are widespread methods by which Man-in-the-Middle Attack executes. To prevent your network from this attack one can use Secure/Multipurpose Internet Mail Extensions (S/MIME) which will ensure that only intended recipients can read or amend the data. And other way is by using Authentication Certificates for all employee machines where only properly configured certificates can get access to systems.

(iii). ***How a Man-In-The-Middle Cyber security Attack Works?[21]:*** MiTM attack is one of the oldest existing attack. This paper explains how MiTM cyber security works and its counter measures to secure any enterprise network. According to this, Vigilance is the preeminent method to evade MiTM attack. One must for all time use encrypted HTTPS.

(iv). ***The Rising Threats to Internet Users [22]:*** This study depicts that MiTM is a snooping attack in which a public key is exchanged by the attacker and is replaced by own public key. This article explains various type of MiTM attack like Man-in-the-IoT, Wi-Fi Eavesdropping, Man-in-the-Cloud, Man-in-the-App, Man-in-the-Mobile and Man-in-the-Browser. One should setup a two-factor authentication on all important keys, use dedicated laptop for online transaction, time to time monitored your accounts for any unusual activity, and always use encrypted versions of online sites these are some measures to prevent from MiTM attack.

(v). ***Man-in-the-Middle (MiTM) Attack [23]:*** The study explains that MiTM attack is the equivalent of a mail carrier opening your personal letters and then writing down some crucial information and then re-sealing the envelope and delivering it to your doorstep. Interception and decryption are two distinct phases of MiTM attack. To prevent from the attack various measures are mentioned that one should look for browser notifications reporting website being unsecured, One should not use public networks and, Wi-Fi that and not password protected.

(vi). ***Man-in-the-Middle attacks on mobile apps [24]:*** This article has focused on MiTM attacks in mobile apps. Malicious proxies can attack easily; they are design to intercepts a request from sender to receiver. MiTM attacks happen in mobile app due to incorrect certificates and using protocols that are not secure. To overcome this issue pinning between the server's hostname and the certificates, and also checking that the certificate is from valid root authority can be used.

(VII). ***Security Attack Issues and Mitigation Techniques in Cloud Computing Environments [25]:*** By reducing the attacks vulnerability and improving the security, one can achieve the effective use of cloud computing. This paper proposes different types of attack that affects cloud environment and various solutions to reduce the attacks. MiTM attack can be avoided by proper authentication mechanism, by using different encryption and decryption mechanism.

(VIII). ***Man-in-the-Middle (MITM) Attacks: Techniques and Prevention [26]:*** This study explains various key techniques which can be used to execute MiTM attack like DHCP MITM, Wireless MiTM, ARP Poisoning, Man-In-The-Browser, Cookie Hijacking, DNS MiTM, and SSL MITM etc.

(IX). ***What is a Man-In-The-Middle Attack? [27]:*** MiTM is an attack, which is in opposition to a cryptographic protocol. This article presents an assortment of implications of the MiTM attack and also provides server keys shield against the MiTM attack. There are three different mode of server key; one is where attacker generate a new server key, second is that the attacker have been able to penetrate the server and steal its server key and the last is attacker is able to generate false certificate. To prevent this X.509 certificate can be used and any kind of proprietary certificates mechanism can be launched.

(x). ***Infosec Guide: Defending Against Man-in-the-Middle Attacks [28]:***MiTM attack is high potential threats that IT experts should be able to concentrate on. To mitigate such attacks one should know different techniques which these attacker uses against users. One of these technique is ARP cache poising to overcome this issue one can add static ARP entries into the cache.

(xi). ***95% of HTTPS servers vulnerable to trivial MiTM attacks [15]:*** MITM attack is highly susceptible to HTTPS server. An attacker can exploit this attack as HTTP connection can easily hijack as no crypto-wizardry required. HTTP Strict Transport Security supports to prevail over MiTM issue but it is not extensively implemented.

(xii). ***TOP four best practices to avoid man-in-the-middle attacks [29]:*** MITM attack has become more widely favoured by cyber criminals. If MITM attack gets successful then a company can face negative perception and can lost faith of their customers.

(xiii). ***Understanding Man-In-The-Middle Attacks SSL Hijacking [30]:*** This article focuses on SSL spoofing which is one of the most potent MITM attack. It exploits the services that people uses and they think that they are secure. Prevention that can be taken from client's perspectives are always do online banking from home, always use HTTPS which are more secure and always have security related software on your server.

(xiv). ***Man in the Cloud Attack Leverages SaaS Vulnerability [31]:*** Cloud data synchronisation is enabled by Software-as-a-service (SaaS) applications. Man in the cloud is an attack on SaaS platform places by which attacker can access on tokens which is more vulnerable than passwords. As tokens are used by the applications so they are more vulnerable because they can't be change frequently to overcome this organisation should more focus on data security.

(xv). ***When three isn't a crowd: Man-in-the-Middle (MiTM) attacks explained [32]:*** This study has provided outline and explained the effective working of Man-in-the-Middle (MiTM) attack. The paper has also highlighted the most common types of Man-in-the-Middle (MiTM). This paper has introduced the new terms like man-in-the-cloud and man-in-the-IoT. The paper has provided various countermeasures for decreasing the failure level.

(xvi). ***How to Secure RDP Sessions from MiTM Attacks [33]:*** This study has focused on the remote desktop protocols, which are used for network communication and remotely accessing the servers and manage the virtual terminals and applications. The study points out the exploitation of the encrypted data channels which are meant to secure the sessions from the attackers. The study has demonstrated the exploitation of vulnerabilities in the encrypted data statistics channel.

(xvii). ***A Review of Man-in-the-Middle Attacks [34]****:* This paper proposed some methods to protect from Man-in-the-Middle man attacks in communication network. It also states that one cannot eliminate this attack completely but can minimize the possibility by some security measures like by host hardening and by designing network from security point of view.

(xviii). ***A Survey on Man-in-the-Middle Attack [35]:*** This paper focuses on the implementation of MiTM attack on Diffie-Hellman and an assortment of measure to reduce this attack. Recent updated operating system (OS) should be used on network system for reducing the risk of Man-in-the-Middle attack.

(xix). ***Man-In-The-Middle-Attack Prevention Using HTTPS and SSL [16]:*** This paper recommended a countermeasure to deal with MiTM attack by proposing the combination of blowfish algorithm AND Diffie-Hellman method. Blowfish for encryption along with DH for key generation enhances the security and minimizes the attack.

(xx). ***Analysis on Man-in-the-Middle Attack on SSL [36]:*** Some of the most important attack in SSL is MiTM attack. MiTM attack confuses user that they are connected to original network or not. Attacker can easily modify the information and forged the data. To deal with this attack one major approach has been made in this paper that is ARP poisoning.

(xxi). ***Defending Man-in-the-Middle Attacks [37]:*** This attack targets directly at the integrity and confidentiality of the information flowing between two servers. The counter measure of MiTM is by blocking the unauthorised user from entering the local file through network. Server can identify and keep track on unauthorised IP address and block that particular IP address.

(xxii). ***An overview of the Man-In-The-Middle Attack [38]:*** According to this paper MiTM is very dangerous as it clearly break the trust between two parties. User thinks that he is communicating to the intended recipient without leakage of any information over a secured network, but attacker can steal\ modify the information without getting caught. This paper focuses on different types of MITM attack.

(xxiii). ***Analysis of MITM attack in Secure Simple Pairing [39]*****:** MITM attacks are generally networked related attacks that hijack a network connection without either of a victim aware of this. This paper proposed the prevention of this attack by introducing an algorithm that detects MITM attack at second stage of SSP i.e. Simple Secure Pairing.

(xxiv). ***Analysis of the Security and Privacy Requirements of Cloud-Based Electronic Health Records Systems [40]:*** This study has focused on the cloud based electronic health records. In this paper the generic service provider security requirements have been analysed in order for the safety of patient files and personal information. The paper has discussed major requirements a health system needs to move on cloud like cloud provider with third party certification, requirement of cloud provider platform to have employee lifecycle policies, platform security, and the most important is the network security safety like Man-in-the-Middle attacks through SSL for server authentication.

(xxv). ***What is a Man-in-the-Middle attack and how can I avoid it? [41]:*** This study has focused on the basic working of Man-in-the-Middle attack. The study has highlighted the protection which exists in system for the prevention from Man-in-the-Middle attack and different features were also pointed for MiTM attack.

(xxvi). ***CCCP: Closed Caption Crypto Phones to Resist MITM Attacks, Human Errors and Click-Through [42]:*** This study has depicted that the use of automated checksum comparison in Closed Captioning Crypto Phones would completely secure the data from MITM and also would decrease the human error compared to traditional approach. The likelihood is also decreased with the use of CCCP. Later the study also focused on the improvement of CCCP using specialized selected transcribes and

checksum of dictionaries for increasing the usability and security.

(xxvii). ***Securing Cloud Computing from Different Attacks Using Intrusion Detection Systems [43]:*** This study aimed to present attack threatening categorization in cloud services and resources on the basis of integrity, confidentiality and availability. The paper research has also provided the related work and review of literature to identify all the categories of attack. This paper has introduces a model called intrusion detection method which identifies and prevents from some of the attacks. One of the attack known as Man-in-the-Middle attack can be easily prevented by intrusion detection method.

IV. CONCLUSIVE FINDING

A significant study of the above reported findings depict that Man-in-the-Middle attack requires major in-depth with respect to Security. Researchers have done extensive work in the threat sphere of influence but still there is a prerequisite to effort additionally in the Man-in-the-Middle attack domain more imperatively.

On the basis of aforementioned survey, diverse sub-areas have been recognized. In view of that, various conclusive finding in the aforementioned domain have been identified and given as follows:

(i). Ontological structured approach is required for conducting the mitigation techniques and threat analysis will unhide the vulnerabilities lying in the cloud [44][45].

(ii). System or technology affected by Man-in-the-Middle attack needs to have a backup plan for resolving the security issues of consumers and providers in cloud.

(iii). Surveillance Mitigation Checklist needs to be developed for the help of end- user security precautions.

(iv). The symmetry between the mitigation techniques and the detecting techniques needs to be ensured for diverse approaches.

(v). There is a need to work on the awareness methods of Man-in-the-Middle attack in cloud for understanding the preventive methods and policies in term of people and technology.

(vi). There are already different security measures for Man-in-the-Middle attack but these are not up-to-date with the new technology. Thus the feasibility level of the security measures of threat need to be examined.

(vii). Network threats are wide in nature and are classified into various threats, which are associated with each other. Therefore the review of each attack with other can provide a new countermeasure for many threats.

(viii). Further study may be worked on empirical/practical aspects of Cloud to investigate the effects of Man-in the-Middle attacks on the resources of cloud.

(ix). There is a need to develop strong wireless access point system and WPAD protocol. More focus is required to be taken on the principles based Wi-Fi networks [10].

(x). There is a need to develop a systematic and structured procedure control on the real-time processing of transactions [11].

(xi). There is a need to understand the proper concepts of how to configure the authentication and Secure socket layer on network [15].

(xii). Restriction regarding free malware, sensitive sites and forged certificates should be taught to the basic service providers and consumers [6].

(xiii). There is a need to work on all the wireless routers, which supports the activities of Man-in-the-Middle attack activities [17].

V. CONCLUSION AND FUTURE WORK

Emerging cloud is majorly getting affected by various threats from network level to application level, which needs to be focused for making the cloud services more secure [46][47]. This research work has highlighted the security problems, root cause and challenges raised due to the Man-in-the-Middle attack. This paper has focused about the defensive mechanisms existing in the cloud environment and reviewed the inclusive and meticulous prior finding from various research studies related to Man-in-the-Middle attack. Through covering various magnitudes of prior survey results, the study points out the major improvements required inconclusive finding for future research directions to provide mitigation techniques for the same. Future research studies may be undertaken to any of the aforementioned research areas. Subsequently, suitable countermeasures may be projected to provide acceptable security to both user and service provider.

Additionally, these attacks and their countermeasures can be implanted in the Cloud Security Ontology (CSO) to current conclusion in way that is more scientific. Another study may be worked to recommend a Surveillance Mitigation Checklist (SMC) for Man-in-the-Middle attack, which will be used for examining the countermeasures and dropping the level of failure to a little extent. The SMC may be based on sectors for further inclusive revision for the organizations. It is expected that future studies will improve confidence and trust in the adoption of Cloud among its different stakeholders.

REFERENCES

[1]. Vaishali Singh & S. K. Pandey, "Research in Cloud Security: Problems and Prospects", International Journal of Computer

Science Engineering and Information Technology Research (IJCSEITR) Vol. 3, Issue 3, Aug 2013, pp. 305-314.
[2]. Vaishali Singh & S. K. Pandey, "Revisiting Cloud Security Issues and Challenges", International Journal of Advanced Research in Computer Science and Software Engineering Vol.3.Issue7, July-2013, pp. 1-10.
[3]. Vaishali Singh & S. K. Pandey, "Cloud Security Related Threats", International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September-2013 pp. 2571.
[4]. Lea Toms, 5 Common Cyber Attacks in the IoT - Threat Alert on a Grand Scale, 29 Apr 2016, GlobalsIGN, Available fromhttps://www.globalsign.com/en/blog/five-common-cyber-attacks-in-the-iot/
[5]. NehaKhandelwal, Chetan Kumar, Security in Cloud: Attacks & Prevention Techniques, International Journal of Latest Trends in Engineering and Technology (IJLTET), Vol. 5 Issue 1 January 2015
[6]. Ricky Publico, What is a Man-in-the-Middle Attack and How Can You Prevent It?, 01 Mar 2017, Available fromhttps://www.globalsign.com/en-in/blog/what-is-a-man-in-the-middle-attack/
[7]. Ramakrishna Thurimella, Leemon C. Baird III, Network Security, Available fromhttp://web.cs.du.edu/~ramki/courses/security/2010Spring/networkSecurity.pdf
[8]. Most Common Wireless Network Attacks, Apr 19, 2018, Cybersecurity Advice, Internet Security, Mobile Security, Network Security, Web Filtering, Available fromhttps://www.webtitan.com/blog/most-common-wireless-network-attacks/
[9]. Martin Vondráček, Jan Pluskal,OndřejRyšavý, Automated Man-in-the-Middle Attack Against WiFi Networks, Journal of digital forensics security and law, Volume 13, Number 1 Article 9, 31 March 2018
[10]. Qi Alfred Chen, Eric Osterweil, Matthew Thomas, , Z. Morley Mao, MiTM Attack by Name Collision: Cause Analysis and Vulnerability Assessment in the New gTLD Era, 2016 IEEE Symposium on Security and Privacy, IEEE Computer Society.
[11]. Neil DuPaul, What Is a Man-in-the-Middle Attack?, Veracode,https://www.veracode.com/security/man-middle-attack,2018
[12]. Jeff Bilger, Holly Cosand, Noor-E-Gagan Singh, Joe Xavier, Security and Legal Implications of Wireless Networks, Protocols, and Devices, https://courses.cs.washington.edu/courses/csep590/05au/whitepaper_turnin/WiFi%20-%20final.pdf
[13]. Alberto Ornaghi, Marco Valleri, Man in the middle Man in the middle attacks, Blackhat Conference - Europe 2003, https://www.blackhat.com/presentations/bh-europe-03/bh-europe-03-valleri.pdf
[14]. Jesudoss A., Subramaniam N.P., A Survey On Authentication Attacks And Countermeasures In A Distributed Environment, Vol. 5 No.2 Apr-May 2014
[15]. Paul Mutton, 95% of HTTPS servers vulnerable to trivial MITM attacks,17th March, 2016, https://news.netcraft.com/archives/2016/03/17/95-of-https-servers-vulnerable-to-trivial-MiTM-attacks.html
[16]. TulikaShubh and Shweta Sharma, Man-In-The-Middle-Attack Prevention Using HTTPS and SSL, IJCSMC, Vol. 5, Issue. 6, June 2016, pg.569 – 579
[17]. Cyber Attacks Explained Man In The Middle Attack, Valency Network, http://www.valencynetworks.com/articles/cyber-attacks-explained-man-in-the-middle-attack.html
[18]. How to Prevent Man in The Middle Attacks, Solid State System LLC, http://solidsystemsllc.com/prevent-man-in-the-middle-attacks/
[19]. Anna, Man In The Middle Attack Prevention And Detection, May 22, 2018, https://www.protectimus.com/blog/MiTM-prevention-and-detection/
[20]. Davey Winder, Man in the cloud attacks, IT Security Things,https://itsecuritything.com/man-in-the-cloud-attacks/
[21]. Christopher Risner, How a Man-In-The-Middle Cybersecurity Attack Works, https://www.blueboltsolutions.com/how-a-man-in-the-middle-cybersecurity-attack-works-3.aspx
[22]. Bill, The Rising Security Threats of 2018, https://blog.eccouncil.org/the-rising-security-threats-of-2018/
[23]. Man in the Middle (MiTM) Attack, Imperva , Incapsula, https://www.incapsula.com/web-application-security/man-in-the-middle-MiTM.html
[24]. Brian Contos, Man in the middle attacks on mobile apps, https://www.csoonline.com/article/3126363/mobile-security/man-in-the-middle-attacks-on-mobile-apps.html
[25]. Subramaniam.T.K, Deepa.B, Security Attack Issues and Mitigation Techniques In Cloud Computing Environments, International Journal of UbiComp (IJU), Vol.7, No.1, January 2016
[26]. Man-in-the-Middle (MITM) Attacks: Techniques and Prevention, https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/
[27]. What is a man-in-the-middle attack?, Symantec, https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html
[28]. Infosec Guide: Defending Against Man-in-the-Middle Attacks, July 27, 2017, https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/infosec-guide-defending-against-man-in-the-middle-attacks
[29]. Top four best practices to avoid man-in-the-middle attacks, Feb 04, 2014,https://www.forcepoint.com/blog/insights/top-four-best-practices-avoid-man-middle-attacks
[30]. Chris Sanders, Understanding Man-In-The-Middle Attacks - Part 4: SSL Hijacking, http://techgenix.com/understanding-man-in-the-middle-attacks-arp-part4/
[31]. Sean Michael Kerner, Man in the Cloud Attack Leverages SaaS Vulnerability, August 5, 2015, https://www.esecurityplanet.com/network-security/man-in-the-cloud-attack-leverages-saas-vulnerability.html
[32]. Jovi Umawing,When three isn't a crowd: Man-in-the-Middle (MiTM) attacks explained, July 12, 2018
[33]. How To Secure RDP Sessions From MiTM Attacks, v2cloud, https://medium.com/@v2cloud/how-to-secure-rdp-sessions-from-cyber-attacks-4482a9f84f79
[34]. Subodh Gangan, A Review of Man-in-the-Middle Attacks, https://arxiv.org/ftp/arxiv/papers/1504/ 1504.02115.pdf
[35]. Kapil M. Jain and Manoj V. Jain, A Survey on Man in the Middle Attack, IJSTE - International Journal of Science Technology & Engineering, Volume 2, Issue 09, March 2016
[36]. Pushpendra Kumar Pateriya and Srijith S Kumar. Article: Analysis on Man in the Middle Attack on SSL. International Journal of Computer Applications 45(23):43-46, May 2012
[37]. Radhika.P, Ramya.G , Sadhana.K , Salini.R, Defending Man In The Middle Attacks, International Research Journal of Engineering and Technology, Volume: 04 Issue: 3, Mar -2017
[38]. Sonia Rachel, Subhashkar S, An Overview of the Man-In-The-Middle Attack, National Conference On Contemporary Research and Innovations in Computer Science (NCCRICS)- Dec 2017
[39]. Praveen Kumar Mishra, Analysis of MiTM Attack in Secure Simple Pairing, Journal of Global Research in Computer Science, Volume 4, No. 2, February 2013

[40]. Joel J.P.C. Rodrigues, Isabel de la Torre, Analysis of the Security and Privacy Requirements of Cloud-BasedElectronic Health Records Systems, Journal of Medical Internet Research, 2013, vol. 15, iss. 7, e148, p.1
[41]. Jon Watson, What is a Man in the Middle attack and how can I avoid it?,Comparitech, October 19, 2017,
[42]. MalihehShirvanian and NiteshSaxena, CCCP: Closed Caption Crypto Phones to Resist MITM Attacks, Human Errors and Click-Through, CCS'17, October 30-November 3, 2017, Dallas, TX, USA
[43]. Omar Achbarou, My Ahmed El kiram, and Salim El Bouanani, Securing Cloud Computing from Different Attacks Using Intrusion Detection Systems, International Journal of Interactive Multimedia and Artificial Intelligence, Vol. 4, No.3
[44]. Vaishali Singh & S. K. Pandey, "Revisiting Security Ontologies", International Journal of Computer Science Issues, Vol 11, Issue 6, No. 1, November 2014 Pg150-159.
[45]. Vaishali Singh & S. K. Pandey, "A Comparative Study of Cloud Security Ontologies" 2014 IEEE 3rd International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions), Page 797-803.
[46]. Vikas Mangotra,, Richa Dogra, Cloud reliability enhancement mechanisms: A Survey, International Journal of Scientific Research in Computer Science and Engineering, Vol.6, Issue.3, pp.31-34 , June (2018)
[47]. P. Santra, An Expert Forensic Investigation System for Detecting Malicious Attacks and Identifying Attackers in Cloud Environment IJSRNSC Volume-6, Issue-5, October 2018

AUTHORS PROFILE

Ms. Vaishali Singh is presently working as an Assistant Professor in the Department of Computer Science, St. Xavier's College, Jaipur, India. She is also pursuing Ph.D. (Computer Science) from Jagannath University, Jaipur. She has an excellent academic background right from the school level. Under the Institute-Industry linkage program, she delivers expert lectures on various areas of Computer Science. She has contributed in many research papers in reputed International journals and national conferences. Her research interest includes: Cloud Security, Cloud Security vulnerabilities, threats and countermeasures, Access control, Identity measurement etc.

Dr. Kavita Bhatia is currently serving as Director in Emerging Technology, Digital Payments & eGovernance group in the Ministry of Electronics and IT (MeitY, Government of India. She is actively involved in the implementation of the Digital Payments, Digital India and National eGovernance Plan (NeGP) across the country. A BSc (Physics) and B Tech (Electronics Instrumentation) from Bombay University. She began her career as Research Assistant in IIT Mumbai and has implemented Nation-wide first project on Smart Card "SMARS" with RBI and IIT Mumbai. Currently Leading a team of professionals for the implementation of various Technical projects of MeitY like Centre for Excellence in IOT, National Centre for AI, Digital Payments, Mobile Seva, eSangam –Interoperability Gateway , Payment Gateway, eSign – Online Digital Signature and Standards etc for the entire Digital India of Govt. of India.

Dr. Santosh K. Pandey is presently working as Scientist 'D'/Joint Director, Ministry of Electronics & Information Technology, Government of India New Delhi. Before joining MeitY, he was a Faculty of Information Technology with Board of Studies, The Institute of Chartered Accountants of India (Set up by an Act of Parliament) New Delhi. Prior to this, he worked with the Department of Computer Science, Jamia Millia Islamia (A Central University) New Delhi and Directorate of Education, Govt. of NCT of Delhi. He has a rich Academics & Research experience in various areas of Computer Science. His research interest includes: Software Security, Requirements Engineering, Security Policies and Standards, Formal Methods, Cloud Computing, Security Metrics, Vulnerability Assessment etc. He has published around 60+ high quality research papers and articles in various acclaimed International/National Journals (including IEEE, ACM, CSI) and Proceedings of the reputed International/ National Conferences (including Springer). Out of these publications, most of them have good citation records. He has been nominated in the board of editors/reviewers of various peer-reviewed and refereed Journals. In addition, he has also served as a Program Committee Member of several reputed conferences in India as well as abroad. He has also been designated in various academic/research committees by the government organizations as well as software companies as a subject expert.

