XSS MBot: Mobile Botnet for Stealthy DDoS Attacks

PMD Nagarjun, Shaik Shakeel Ahamad

Abstract*: Mobile devices are overgrowing; nowadays people are using mobile devices for different activities. Over the years malware attacks on mobile devices are increasing, the primary intention of the attacker is to steal sensitive information and turn the infected mobile device into a member of the botnet. We studied differences between traditional botnets and mobile botnets, also analyzed different mobile botnet attacks. Mobile malware applications spread through Cross-site Scripting vulnerabilities in trusted websites. Developed a mobile malware which can perform Denial-of-service attacks and used this malware to test and review mobile botnet attacks. We also studied solutions to prevent these mobile botnet attacks.

***Index Terms*: Android Application, Cross-site Scripting, Mobile Botnets, Mobile Malware.**

I. INTRODUCTION

Mobile phones are getting powerful every day, and these smartphones are having processing power almost equal to regular desktops or laptops. People are spending a high amount of time on mobile phones for daily activities. Internet availability on mobile phones overgrowing through either 3G/4G or Wi-Fi connections. Mobiles are used to perform bank transactions, send messages and sensitive data transfer in the form of E-mails, etc.

According to GSMA Intelligence, in 2017 there are 5 billion unique mobile subscribers around the world, and 3.3 billion mobile internet users.

Most popular mobile operating systems are Android and iOS. Compared to iOS 86%, only 11% of Android mobile users having the latest updates of operating systems. Attackers can exploit vulnerabilities in old operating systems.

With the growth of mobile devices, attacks on mobile devices also increased. If an attacker manages to install malware on the mobile device, then the attacker can steal sensitive information from mobile devices, send or receive unwanted SMS messages and can turn the mobile device into a bot in the botnet. Mobile bots can perform distributed denial-of-service (DDoS) attacks on targets by following orders from the botmaster.

In this paper, some of the popular botnet attacks are studied and implemented a botnet to perform DDoS attacks. Developed a mobile malware application which can turn a mobile device into a bot. As a bot in the botnet, the mobile device can perform denial-of-service (DoS) attacks based on botmaster request and discussed solutions to prevent botnet attacks. This paper is structured as follows. Section 2 discusses the literature work. Section 3 describes the botnet attacks. Section 4 discusses the proposed botnet. Section 5 discusses solutions to prevent botnets, and section 6 provides the conclusion.

II. LITERATURE WORK

Karim et al. [1] studied Botnets in mobiles, which operates on a command and control (C&C) architecture. Their study shows the evolution of Botnets from traditional PC to mobiles. According to their study, the main constraints for mobile devices are 1. Battery power, 2. Application usage cost, 3. Communication cost, and 4. Communication complexity. And Android is the most malware affected the mobile platform. According to them the insecure boot, improper input validation, user knowledge, and SIM flaws are causes of most malware mobile attacks.

Khana et al. [2] studied different security-related challenges for mobile users, mobile threats, mobile vulnerabilities. Different types of mobile risks involved in their study are physical based threats, application-based threats, network-based threats, and Web-based threats. A botnet is one of serious money related threat in all mobile vulnerabilities. According to them one of important security defense mechanism for data privacy and mobile security is Biometric authentication. Security mechanisms need to be involved in every stage of mobile application development.

Agasi [3] stated that there is no complete solution to prevent mobile security problems. The main issues with mobile security are implementing proper security policies, integrating current security and protecting data in mobile devices. To provide adequate protection to business documents and data, the corporate need to implement the secure environment for mobile devices, threat management, and security policies need to be independent of devices and operating system used in them.

Hua & Sakurai [4] implemented an SMS based mobile botnet. Which uses SMS to send command and control messages to bots. To improve the stealthiness of SMS botnet, they encrypted the messages. Wi-Fi is more stealthy compared to the cellular network. Their work shows that by using Erdos-Renyi random graphs topology in the botnet, they can send the command from botmaster to 90% of bots (total 20000 bots)

Revised Manuscript Received on July 09, 2019

PMD Nagarjun, Department of CSE, K L University, Guntur, India.

Shaik Shakeel Ahamad, Department of Information Technology, CCIS, Majmaah University, Al Majmaah, Kingdom of Saudi Arabia and Department of CSE, K L University, Guntur, India.

with no more than 4 SMS within 20 minutes. They also discussed different defensive methods to prevent this type of SMS botnet attacks, one of them is to implement hardware notification whenever an SMS was sent or received.

ByungHa [5] proposed a botnet detection method by using a VPN. All traffic between bot device and C & C server will go through VPN IDS, and VPN IDS will detect malicious packets. Their proposed method identifies pull style command and control channel between a bot and C & C server. Their proposed schema detects botnets with white list, signatures and abnormal models. They tested their schema by installing 11 bots and able to identify 94.6-100% of botnet attacks.

Xiang et al. [6] proposed a botnet named Andbot which works on Command and Control mode. Andbot targets Android mobile operating systems. Andbot uses cache mechanism to reduce resource consumption. Features of Andbot were stealthy, resilient and low cost. Andbot uses HTTP based URL Flux protocol to access the internet.

III. BOTNET OVERVIEW

A botnet is a collection of infected devices [7] which are connected to the internet and controlled by single or multiple entities. Fig. 1 shows a simple client-server structure of a botnet.

Over the years the gap between mobile devices and personal computers are narrowing. The same architecture of traditional botnets will also work on mobile devices, and bots are infected mobile devices [8].

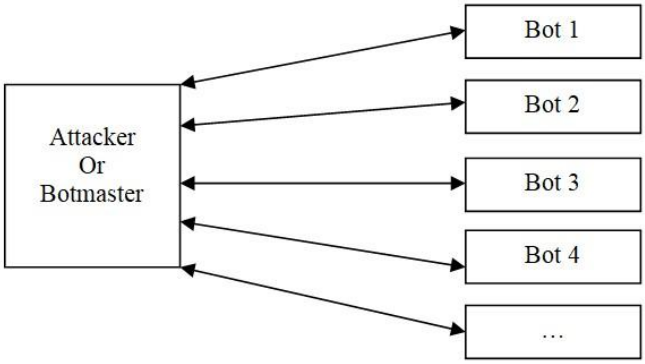

Fig. 1 Botnet structure client-server model

A. Spreading Mobile Malware Applications by Cross-site Scripting Attacks

Cross-site scripting (XSS) attacks are one of the severe attacks on Web applications [9] and Hybrid mobile applications [10]. An attacker exploits XSS vulnerabilities in the trusted website and modifies the web page in the way that it will ask visitors to install malware infected mobile app like fig. 2. And attacker share that attacked web page URL in sharing apps.

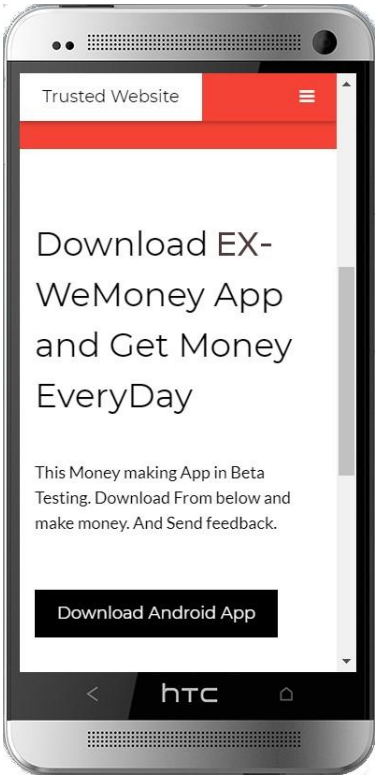

Fig. 2 Trusted website with fake app advertisement

Sharing is a popular activity in mobile devices, mobile users frequently share personal and interesting information to family, friends. If they receive a link to a trusted website with an interesting title, they will share without validating the link. And even open the link and install malware mobile app because it is suggested by the trusted website and may become part of a mobile botnet. Fig. 3 shows how malware spreads through sharing between mobile users.

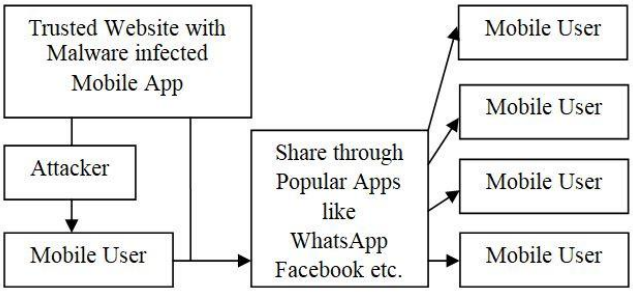

Fig. 3 Mobile malware spread through XSS vulnerability in a trusted website

B. Popular Android Mobile Botnet Attacks

DroidDream: This Trojan [11] gets unique identification information of mobile phone by gaining root access. It can download malicious code and gives full control of the mobile phone to the hacker. More than 50 infected Android apps identified in the official Android marketplace. Google manages to remove infected Apps from the Android marketplace by using the kill switch mechanism.

Geinimi: This data stealing Android Trojan [12] emerged in China. After infecting the mobile device, this Trojan can send a list of installed apps, location details and unique identification number information to the remote server. This Trojan distributed through mobile games. Geinimi Trojan can be avoided by resetting registry information of mobile phones. Geinimi Trojan uses obfuscation and encryption to hide its functionalities.

C. DDoS attacks by using Mobile Botnet

Attackers can steal sensitive information [13] from infected mobile bots and possible to send malicious messages. The attacker can use a group of infected mobile bots to perform DDoS attacks on websites. Fig. 4 show the DDoS attack by using Client Server botnet model. In DDoS attacks, botmaster issues a command to bots in the botnet to perform an attack on the targeted website.

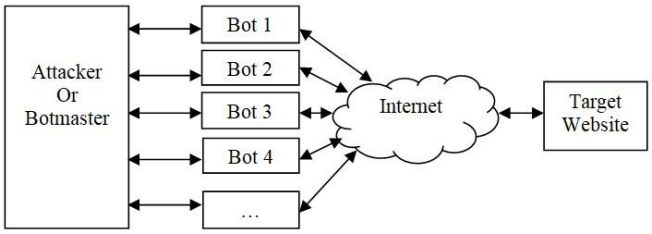

Fig.4 DDoS botnet attack

D. Command and Control Channel

In the centralized botnet, there are two styles of Command and Control (C&C) [14] channels. C&C channels decide how botmaster communicates with infected bot devices. Table 1 shows two styles of C&C channels. Fig. 5 and Fig. 6 shows how communication happens between bots and botmaster in two forms of C&C channels.

Table. 1 Comparision C&C channels in a centralized botnet

Method	Protocols Used	Who Starts Communication
Push Style	IRC	Botmaster
Pull Style	HTTP	Bot

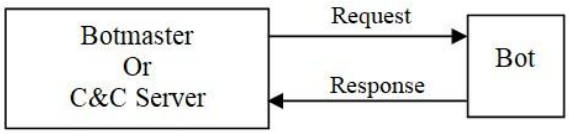

Fig. 5 Push style C&C channel

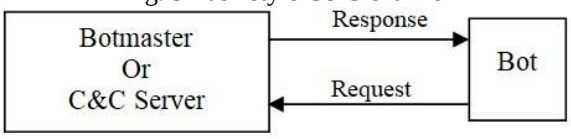

Fig. 6 Pull style C&C channel

IV. XSS MBOT - PROPOSED MOBILE BOTNET

Proposed Cross-site Scripting Mobile Bot (XSS MBot) uses Pull style Command and Control [15] channel for communication between infected bots and botmaster. In this botnet, an attacker shares malware mobile apps to users by exploiting Cross-site Scripting vulnerability in trusted websites. Fig. 7 shows the architecture of proposed botnet and fig. 8 shows how commands flow between botmaster, zombie master, zombie slave, and mobile bot. Botmaster can issue commands to bots regarding targets [16] to attack through zombie slaves. This botnet can do distributed denial-of-service (DDoS) attacks [17] on specified targets.

XSS MBot targets Android mobile phones. Ones, an infected Android application installed on the mobile device it will communicate with predefined zombie master. Zombie master contacts botmaster and registers infected mobile bot at botmaster. Botmaster assigns a unique ID and provides a list of zombie slaves [18] to every mobile bot through zombie master, and this unique ID used in communications. Mobile bots communicate periodically with zombie slaves to know the target website to attack.

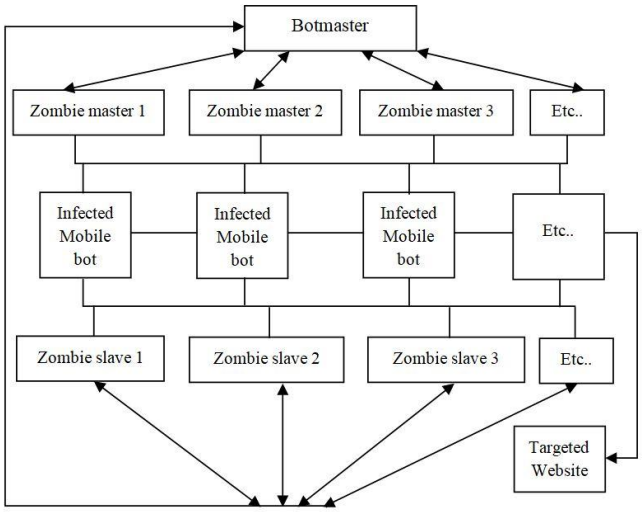

Fig. 7 XSS MBot - Mobile botnet architecture

Botmaster communicates with zombie slaves and sets the target website to perform the DDoS attack. After providing the target website to the mobile bot, zombie slave set the status of the mobile bot at botmaster by using the unique ID.

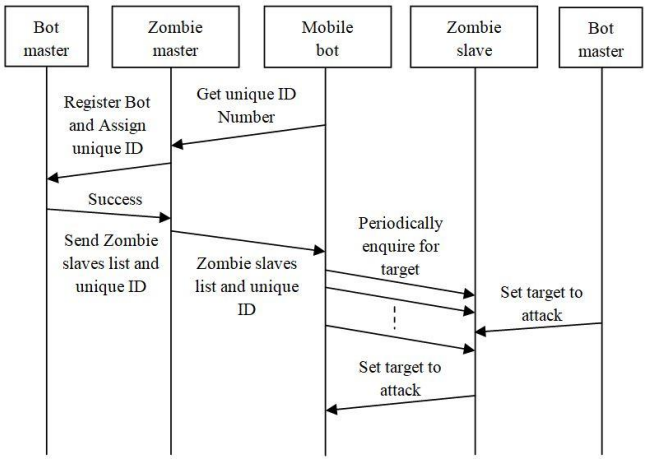

Fig 8. XSS MBot - Commands flow

To achieve stealthiness and randomness communications between bots [19], zombie master and zombie slaves encrypted with random passwords. These random passwords are simple texts and selected by infected mobile bots.

A. XSS MBot URL Formats

Fig. 9 shows infected mobile bot request to zombie master, the request URL contains https as protocol, one of random zombie master as the host-name and random page with a random encrypted data in the query string.

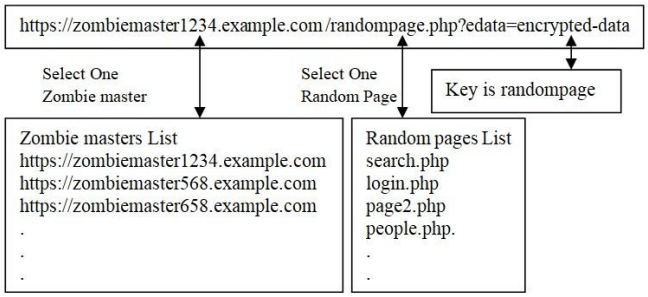

Fig. 9 Mobile bot to zombie master URL format

Fig. 10 shows infected mobile bot request to zombie slave, the request URL contains https as protocol, one of random zombie slave as the host-name and random page with an encrypted unique ID in the query string.

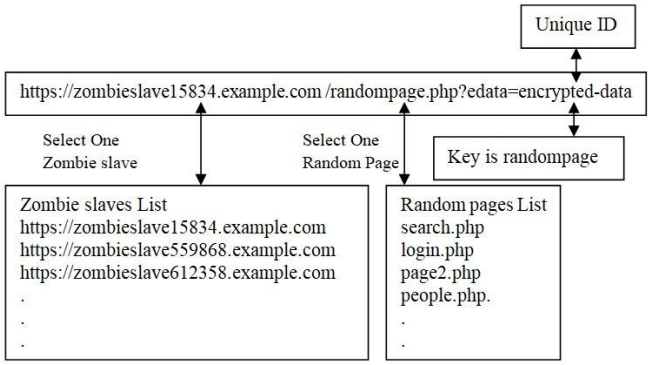

Fig. 10 Mobile bot to zombie slave URL format

B. Infected Android Application

We created a simple Android application named EasyNotePad with attack code to test botnet. This app requires permissions like Internet and Storage. The android application is a simple notepad type application, and it can be used to store notes, edit old notes and delete notes. Fig. 11 shows the infected android application, but malicious activity happens in the background.

After installing this app, a background service will be created. First, it will contact the zombie master and get the unique ID and zombie slaves list. Mobile bot communicates periodically with zombie slaves to know the target. After getting the target to attack, it will send simple HTTP requests to target periodically, and it will stop attacking when the botmaster stops the attack. Fig. 12 shows how botmaster sets the target to attack and know the current status of mobile bots.

Status "waiting" means mobile bot ready to attack and status "attacking" means mobile bot currently attacking the target. If botmaster set the target to "no" means stop the current attack. We can perform the DDoS attack on a specified target by installing this infected app on real Android mobile devices.

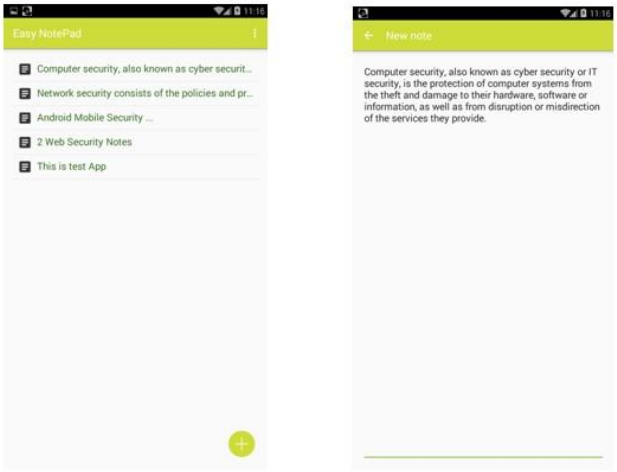

Fig. 11 List of notes and adding a new note in EasyNotePad app

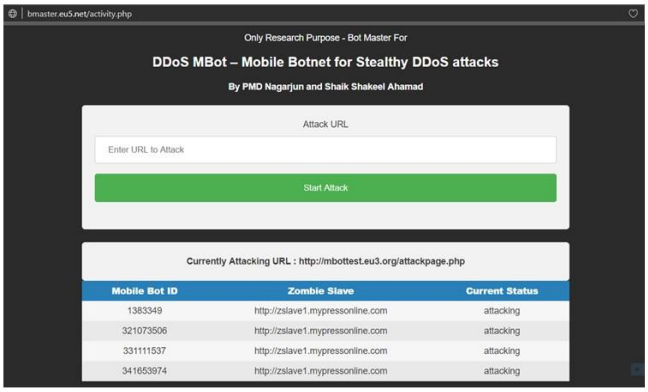

Fig. 12 Botmaster setting target to attack

V. SOLUTION TO AVOID THESE TYPE OF BOTNET ATTACKS

These type of botnet attacks are difficult to detect because the malicious activity of infected applications is insufficient, so behavior-based detection systems may fail to recognize this botnet activity. Installing applications from trusted sources or applications of trusted companies will avoid these type of infected apps, which causes botnet attacks. By analyzing internet traffic on a mobile device, this type of botnet attacks can be detected and prevented.

VI. CONCLUSION

Mobile devices are vulnerable to malware attacks. Infected mobile devices may act as a bot in botnet and attacker can use that infected mobile device to perform the DDoS attack. The attacker can spread infected apps through Cross-site Scripting attacks in trusted websites. XSS MBot botnet is proposed and implemented to perform DDoS attacks on specified targets by using Mobile devices as bots. Created Malware-infected Android app named EasyNotePad and discussed spreading of this Malware app through Cross-site Scripting attacks. Proposed botnet involves different entities like botmaster, zombie master, zombie slave, and mobile bot. Based on botmaster command zombie slaves set the attack target, and mobile bots attack those targets. Preventing these types of botnet attacks is difficult, effective solutions are installing apps from trusted sources and proper analysis of mobile traffic to detect botnet activity.

REFERENCES

1. A. Karim, S. A. A. Shah, R. B. Salleh, M. Arif, R. M.Noor, and S. Shamshirband, "Mobile botnet attacks an emerging threat: Classification, review and open issues.,"TIIS, vol. 9, no. 4, pp. 1471–1492, 2015.
2. J. Khan, H. Abbas, and J. Al-Muhtadi, "Survey on mobile user's data privacy threats and defense mechanisms," Procedia Computer Science, vol. 56, pp. 376–383, 2015.
3. O. Agasi, "Encapsulating mobile security," Computer Fraud & Security, vol. 2015, no. 6, pp. 10–12, 2015.
4. J. Hua and K. Sakurai, "A sms-based mobile botnet using flooding algorithm," in IFIP International Workshop on Information Security Theory and Practices, pp. 264–279, Springer, 2011.
5. B. Choi, S.-K. Choi, and K. Cho, "Detection of mobile botnet using vpn," in Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2013 Seventh International Conference on, pp. 142–148, IEEE, 2013.
6. C. Xiang, F. Binxing, Y. Lihua, L. Xiaoyi, and Z. Tianning, "Andbot: towards advanced mobile botnets," in Proceedings of the 4th USENIX conference on Large scale exploits and emergent threats, pp. 11–11, USENIX Association, 2011.
7. Wikipedia, "Malware." https://en.wikipedia.org/wiki/Malware, 2017.
8. Wikipedia, "Mobile malware." https://en.wikipedia.org/wiki/Mobilemalware, 2018.
9. I. Hydara, A. B. M. Sultan, H. Zulzalil, and N. Admodisastro, "Current state of research on cross-site scripting(xss) a systematic literature review," Information and Software Technology, vol. 58, pp. 170–186, 2015.
10. W. Bao, W. Yao, M. Zong, and D. Wang, "Cross-site scripting attacks on android hybrid applications," in Proceedings of the 2017 International Conference on Cryptography, Security and Privacy, pp. 56–61, ACM, 2017.
11. T. Bradley, "Droiddream becomes android market nightmare." https://en.wikipedia.org/w/index.php?title=Mobilemalware&oldid=772698711, 2011.
12. T. Strazzere and T. Wyatt, "Geinimi trojan technical tear down,"Lookout Mobile Security, 2011.
13. F. Mercaldo, C. A. Visaggio, G. Canfora, and A. Cimitile, "Mobile malware detection in the real world," in Software Engineering Companion (ICSE-C), IEEE/ACM International Conference on, pp. 744–746,IEEE, 2016.
14. G. Gu, J. Zhang, and W. Lee, "Botsniffer: Detecting botnet command and control channels in network traffic," 2008.
15. Y. Zeng, K. G. Shin, and X. Hu, "Design of sms commanded-and-controlled and p2p-structured mobile botnets," in Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks,pp. 137–148, ACM, 2012.
16. M. Eslahi, R. Salleh, and N. B. Anuar, "Bots and botnets: An overview of characteristics, detection and challenges," in Control System, Computing and Engineering (ICCSCE), 2012 IEEE International Conference on,pp. 349–354, IEEE, 2012.
17. N. Hoque, D. K. Bhattacharyya, and J. K. Kalita,"Botnet in ddos attacks: trends and challenges," IEEE Communications Surveys & Tutorials, vol. 17, no. 4,pp. 2242–2270, 2015.
18. M. Anagnostopoulos, G. Kambourakis, and S. Gritza-lis, "New facets of mobile botnet: architecture and evaluation,"International Journal of Information Security,vol. 15, no. 5, pp. 455–473, 2016.
19. S. Zhao, P. P. Lee, J. Lui, X. Guan, X. Ma, and J. Tao,"Cloud-based pushstyled mobile botnets: a case study of exploiting the cloud to device messaging service," in Proceedings of the 28th Annual Computer Security Applications Conference, pp. 119–128, ACM, 2012.

AUTHORS PROFILE

PMD Nagarjun is Research Scholor in Department of CSE, K L University, Guntur, India. He received his B.Tech in Computer Science and Engineering from JNTU Anantapur and received M.Tech in Information Technology (Networking) from VIT University, Vellore. His research interests are Network Security and Artificial Intelligence.

Dr. Shaik Shakeel Ahamad is currently working as an Assistant Professor in Department of Information Technology, CCIS, Majmaah University, Al Majmaah, Kingdom of Saudi Arabia. He was a Professor in the Department of CSE, KL University, Guntur, India (now on lien). He holds a PhD in Computer Science from the University of Hyderabad, India in the realm of secure mobile payments protocols and formal verification. His research interests are Information Security, Cloud-based Mobile commerce, Secure Mobile Healthcare Frameworks and Protocols, Wireless public key infrastructure and Digital Forensics.