# PERFORMING THE COMPARATIVE ANALYSIS OF DDOS ATTACK IN SIMULATED ENVIRONMENT

**[1]Deepika, [2] Dr. Harmandeep Singh**
[1]Research Scholar, [2]Assistant Professor
[1]Department of Computer Science & Engineering,
[1]Punjabi University, Patiala, India

***Abstract: Penetration Testing is one of the most important part of organization information security. Distributed Denial of Service (DDoS) attack inflict a severe threat to the widely utilized internet based services like e-commerce, e-banking, transportation, medicine, education etc. Hackers exploit the system vulnerabilities for implementing DDoS attacks in order to debase or completely crash the services. In current years, DDoS attacks have been increased in numbers. Despite the fact that a no. of solutions have been proposed against DDoS attacks but still protection from a DDoS attack is a challenging issue. Also hackers are constantly upgrading their skills for developing new advanced attack tools. This paper highlights some of the important DDOS attack methods, tools and simulates an attack over a website running on a local host. It includes the implementation of DDOS attacks, how to use them and create botnets to attack some website. Different types of attacks i.e. HTTP Flood, ICMP Flood and TCP SYN Flood can be implemented using the tools which have been used in this paper.***

***IndexTerms – DDOS, HTTP, Web Server, HOIC, Hping, Nping, Xerxes***

## I. INTRODUCTION

Internet was emerged in early 1990's and got commercialized in 1995 and become interactive that changed the communication system. With each passing day internet is becoming a crucial part of industry and everyday life. Organizations use the client-server architecture for the transmission of data and security of this data is major concern. With the advancement of internet more and more users started connecting to it, that did not have any impact on internet performance but there is one issue that internet has and that is security. Hacker communities around the world use different attacks to exploit any vulnerabilities in the organization applications running over the Internet. DDoS attacks are one of the most common attacks which are mainly used to disrupt the availability of the application of any organization running over the Internet. Botnets are used by the attackers to disrupt the services of the target web application. DDoS attacks are implemented through the well organized, distributed and remotely controlled network so that compromised computers (called zombies or bots) can be used for sending continuous massive attack requests to the target system(s).[1]

DDoS attacks are difficult to detect as they may seem as genuine packets and also as they are coming via botnet, therefore it's very difficult to detect the attacker. Due to these difficulties in detection of the attacker and attack, it is mostly used by attackers to disrupt the network infrastructures of the organizations. DDoS can also be used as a distraction by the attackers while they have a different motive, they may want companies to get confused that it is a DDoS attack to disrupt the network resources, but the target is tricked by hackers to steal the data from their data centers. A very prime example of this sort of attack is when a small ISP from London named "Talk Talk" was attacked by the hackers. Hackers performed a DDoS attack on Talk Talk and suddenly their web services were disrupted and the accessibility of their website was disrupted. All the Talk Talk network team went on to troubleshooting the DDoS attack and put their all focus on resolving that issue while attackers get entry through the backdoor link and steals the customer records from Talk Talk Data Center.

DDoS attacks are increasing every year with attacks over 50Gbps are detected by various service providers. Due to emergence of Cloud and IoT, botnet is becoming more powerful and hackers get the bigger playground to play with. Mirai Botnet [20], which is one of the largest botnet ever, was created with the help of routers and Security Cameras. Some of the major targets of Mirai Botnet was cloud related services like DNS provider Dyn. This, along with millions of MongoDB databases which were hosted in the cloud. According to Symantec, average organizations use around 900 cloud based applications, while their CIOs think they are using around 30, which leads to large scale of inconsistency and underestimated level of risk. Attack on Dyn[16][18], also affects large scale companies like Paypal, Netflix and Spotify.

According to Symantec threat report 2017[20], the Necurs botnet was one of the main distributors of malware in 2016 and was responsible for massive email campaigns distributing JavaScript, VBS, and Office macro downloaders. Necurs primary payload in 2016 was Ransom.Locky. Other major botnets observed by Symantec were used to spread threats such as Dridex (W32.Cridex), Cerber (Ransom.Cerber), and Kotver (Trojan.Kotver), as well as Locky.

## II. DDoS Attack Types

There are three major types of DDoS attacks :

- ***Application Layer DDoS attack:*** These are the attacks[8] which target Softwares like Apache, Windows IIS, or other software vulnerabilities to generate an attack and disrupt the services.
- ***Protocol DDoS attack:*** These types of attacks[15] are made at the protocol level. It includes TCP SYN Flood, Ping of Death etc.
- ***Volume Based DDoS attack:*** This type of attack uses ICMP Floods, UDP Floods, etc via spoofed packets.[8]

Some of the most commonly used DDoS attack types include:

1. ***UDP Flood:*** It is a DDoS attack that targets with the help of UDP packet flooding. It attacks by flooding on random pots on a remote host. This makes host repeatedly checks for the application running on that ports and then reply with the Destination

Unreachable message. This type of attacks can be made on applications using UDP like Video Conferencing Services and conference application can be disrupted using UDP Flood attack[8].

2. ***ICMP (Ping) Flood:*** It is pretty much similar to UDP Flood attacks, it creates a ICMP Request flood and send it to the target machine. This type of attack mainly utilize both outgoing and incoming bandwidth, therefore they are mainly performed using botnets. This type of attack can work on almost all the applications to choke the bandwidth of the network resources[10].
3. ***SYN Flood:*** In TCP SYN Flood attack, attacker sends SYN Floods[10] to the target machine and target machine replies back with the SYN-ACK and needs a TCP ACK in return from the attacking machine, but attacker never sends that back which results in target machine stucks in waiting state for all the TCP 3-Way Handshakes. It can be used to choke down applications running TCP based applications.
4. ***Ping of Death:*** In Ping-of-Death attack, attacker sends flood of malicious pings to the target machine. Attacker sends maximum sized IP packets to the target and it is split over multiple fragments and on the target end, he has to reassemble all the packets and when the target ends up with reassembling of packets, it ends up with packet size larger than 65535 bytes(maximum packet size) and slowly overflow memory buffers are allocated to the packet resulting in DoS attack[9].
5. ***HTTP Flood:*** In HTTP Flood attack, hacker exploits the target by sending HTTP GET or POST requests to web server or web application. This attack requires less amount of bandwidth than other attacks. Target Machine can be choked by sending hundreds of requests or by sending lots of Post messages which can disrupt the services of the web application or web site by choking the bandwidth[10].

## III. IMPLEMENTATION

In this paper HPing3, HOIC, Nping and Xerxes are used in a simulated environment where two virtual machines are created, one is running as Windows XP with XAMPP server installed on it and other one is running as Kali Linux. A website of Punjabi University i.e. www.punjabiuniversity.ac.in has been copied using HTTRACK Website Copier and added to the apache server under XAMPP server. On windows7 HOIC is installed and on Kali Linux  Xerxes, Hping and Nping are installed.  So, mainly the attack is performed on Punjabi university website simulated under a VM1. IP Address of the VM1 running target website is 192.168.204.128 and used HOIC, Hping3, Nping and Xerxes to attack the website.

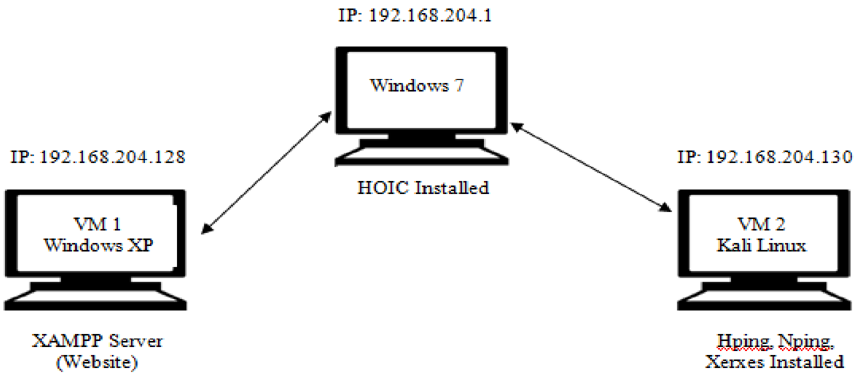

fig 3.1: Overview of attack scenario

Tools used for launching the attack on 192.168.204.128(website) are explained following:

***HOIC –*** High Orbit Ion Cannon is an open source environment to test network stress by flooding target web systems with HTTP GET and POST requests. The attack started on website over port 80 and with power set to high and status is engaging. 74 bots are used to create a botnet for attack. After around 15-16 seconds, attack starts to slow down the website response and after around 30seconds, the website goes down.

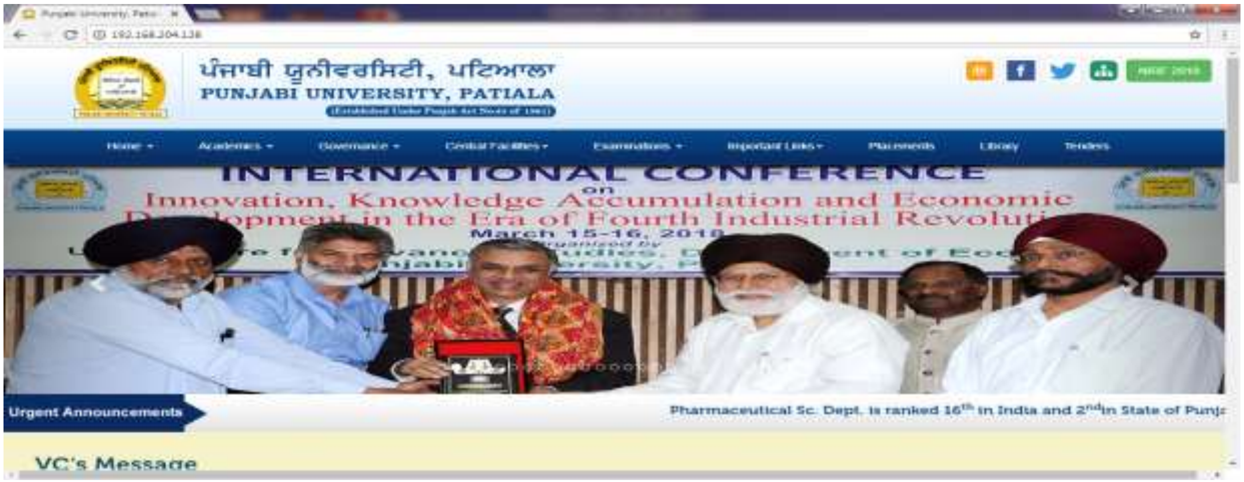
192.168.204.128
ਪੰਜਾਬੀ ਯੂਨੀਵਰਸਿਟੀ, ਪਟਿਆਲਾ
PUNJABI UNIVERSITY, PATIALA
Home
Academics
Governance
Central Facilities
Examinations
Important Links
Placements
Library
Tenders
INTERNATIONAL CONFERENCE
on
Innovation, Knowledge Accumulation and Economic
Development in the Era of Fourth Industrial Revolution
March 15-16, 2018
Urgent Announcements
Pharmaceutical Sc. Dept. is ranked 16th in India and 2nd in State of Punj
VC's Message

fig 3.2 – website to be attacked.

***Hping* –** hping3 is a command line based tool and can be used to create large scale DDOS attacks with random sources. Hping uses the command: hping3 **–**V –c 100000 –d 120 –S –w 64 –p 80 –s 445 –flood –rand-source 192.168.204.128 to start the attack.

HPing performs TCP SYN flood attack on 192.168.204.128, running the website and it slows down the website in around 10 seconds and disrupt the total web services in around 35 seconds.

***Nping-*** Nping is a command line tool and uses the command: nping –tcp-connect –rate 150000 –c 150000000 –q 192.168.204.128 to attack the website. Nping takes more time than hping as the web server slows down the services after around 30 seconds and complete website goes down by around 60 seconds.

***Xerxes*:** Xerxes has to be explicitly downloaded first and then is needed to be compiled using gcc compiler, which then creates a complied file. After that we can send a HTTP flood attack using this command: ./xerxes 192.168.204.128 80, on website over port 80 which slows down the site after around 10second and takes down the whole website in around 25 seconds, which is extremely fast.

## IV. RESULTS AND DISCUSSION

So after all the attacks and tools used for, a table is created that shows the comparative analysis of the tools:

| Tool Name | Operating System Supported | Attack Type | Slows Down Service (Time in seconds) | Website becomes unavailable(Time in seconds) | Interface Type |
|---|---|---|---|---|---|
| High Orbit Ion Cannon | Windows, Linux | HTTP | 15 | 30 | GUI |
| Xerxes | Linux, Windows | HTTP | 10 | 25 | CLI |
| Nping | Linux, Windows | TCP | 30 | 60 | CLI |
| Hping | Linux, Windows | TCP | 10 | 35 | CLI |

table 4.1 – DDOS tool and attack comparison

The above table shows the comparative analysis of the tools being used to attack the website running on 192.168.204.128. According to the implementation of attacks, tools can be compared into two major aspects such as service slow down time and website crash time. Service slow down time is the time at which there is a delay in opening a website. The second one is website crash time i.e the time when website becomes totally unavailable to the user.

The following figures depict the graphical representation of comparative analysis results:

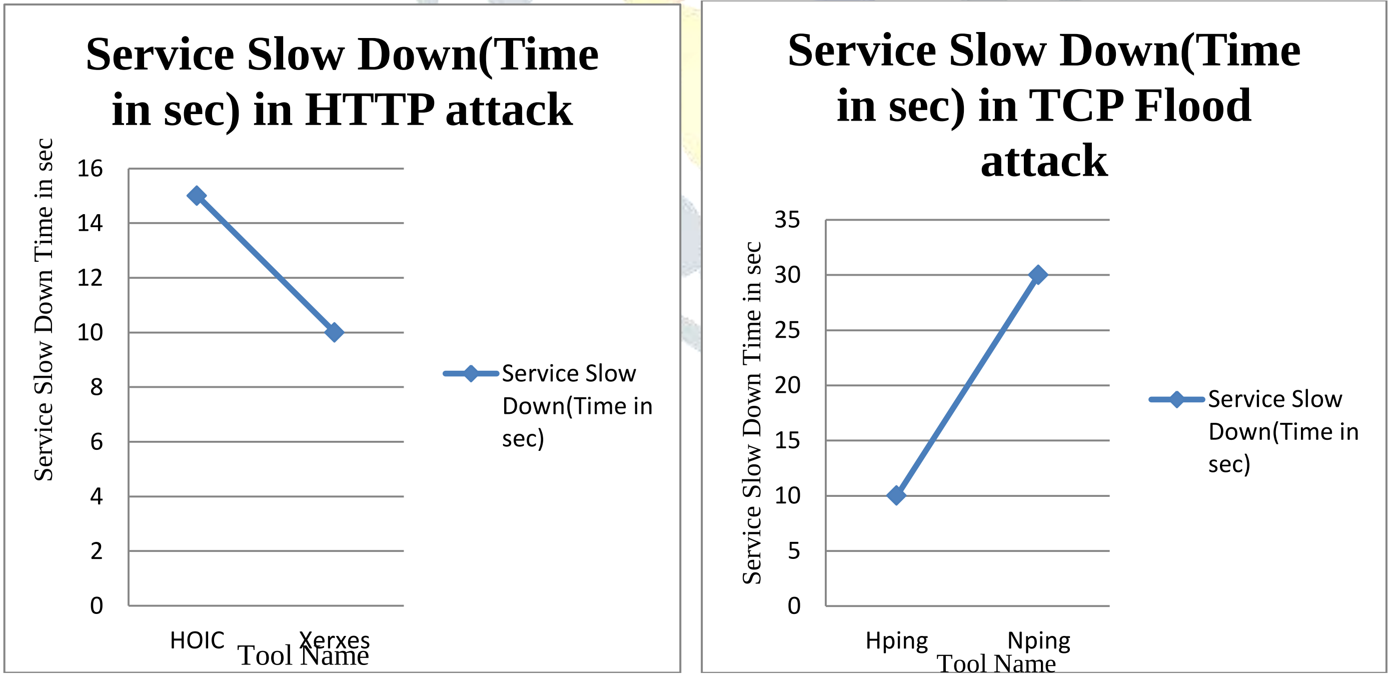

fig 4.1: service slow down graph

The above fig 4.1 depicts the service slow down time of tools according to there attack type. The first graph in fig 4.1 is of HTTP attack performed by HOIC and Xerxes and the second graph is of TCP flood attack performed by Hping and Nping. The X-axis in both the graphs have tool name and the Y-axis have service slow down time. Both graphs shows that Xerxes and Hping are more fast in slowing down the service as compared to HOIC and Nping respectively. Xerxes and Hping slows down the service in 10 seconds whereas HOIC took 15 seconds and Nping took 30 seconds.

Below Figure 4.2 depicts the website crash time graph in which the X-axis has the Tool names and Y-axis has the website Crash time (in sec). First graph formed by HOIC and Xerxes by launching HTTP attack on website shows that Xerxes is more powerful tool than HOIC.

The second graph formed by Hping and Nping by performing TCP flood attack on website depicts that Hping crashed the website faster than Nping.

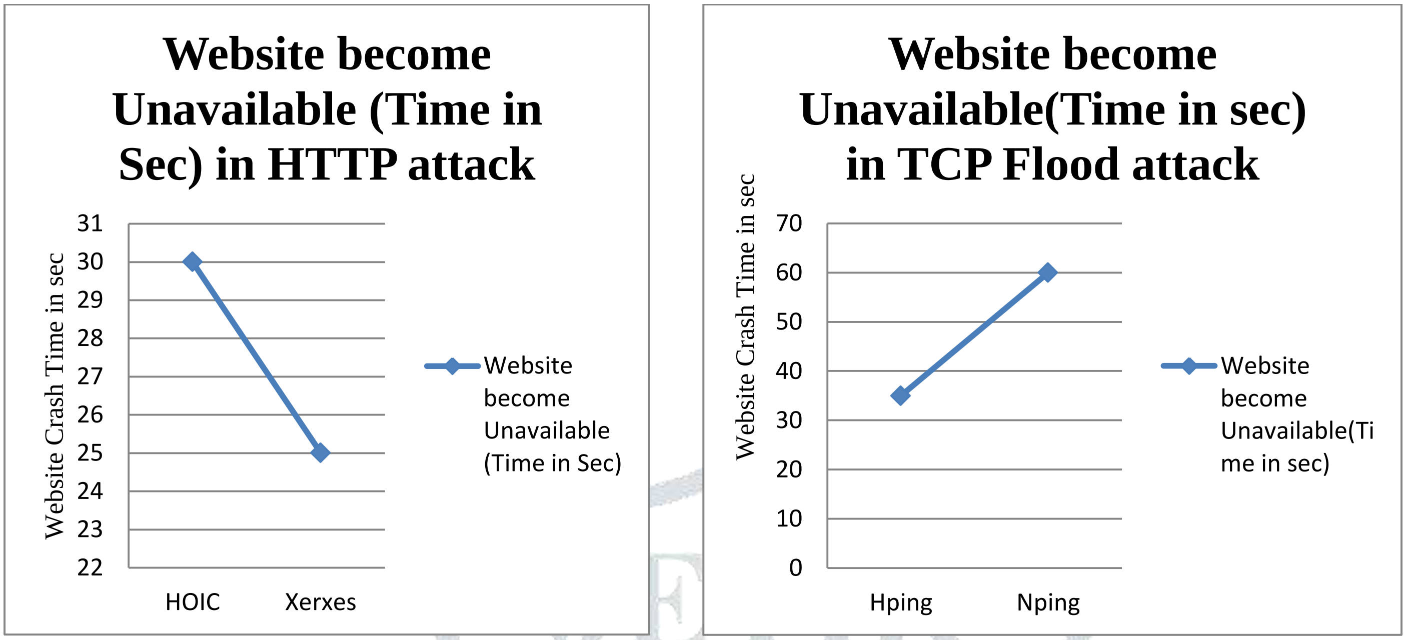

fig 4.2: website crash graph

## V. CONCLUSION

DDOS attacks are rising with every passing day. DDOS tools that are used in this paper can be utilized for performing penetration testing with DDOS attacks to find out the network issues. DDOS attacks can be launched using different methods which can be either TCP SYN Flood, HTTP Flood, or ICMP Flood method. HOIC creates a botnet network that performs the DDOS and takes down the website in around 30 seconds. Xerxes and HOIC both are used for HTTP attack. Comparing the two, Xerxes crash the site faster within 25 seconds. Hping and Nping both are used for TCP SYN flood attack. From these two, Hping crash the site faster within 35 seconds. Out of all the tools tested, HOIC works on a graphical interface whereas Xerxes, Hping and Nping Works on command line interface.

**REFERENCES**

[1] Behal, S., & Kumar, K. (2017). "Characterization and Comparison of DDoS Attack Tools and Traffic Generators - A Review". *International Journal of Network Security* , *19* (3), 383-393.

[2] Denis, M., Zena, C., & Hayajneh, T. (2016). "Penetration Testing:Concepts, Attack Methods and Defence Strategies". *Long Island Systems, Applications and Technology Conference(LISAT).* IEEE.

[3] E., C. (2010). *"Botnets: To what extent are they a threat to information security?"*. . E. Claire, "Botnets: To what extent are they a threat to information security?," Information Security Technical Report, vol. 15, pp. 79-103, 2010. https://doi.org/10.1016/j.istr.2010.11.003. Information Security Technical Report.

[4] Goel, J. N., & Mehtre, B. (2015). "Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology". *3rd International Conference on Recent Trends in Computing 2015(Elsevier)* (pp. 710-715). Procedia Computer Science 57.

[5] H. Bhuyan, M., Kashyap, H. J., Bhattacharyya, D. K., & Kalita, J. K. (2014). "Detecting Distributed Denial of Service Attacks: Methods, Tools and Future Directions". *The Computer Journal* , *57* (4).

[6] Hansman, S., & Hunt, R. (2005). "A taxonomy of network and computer attacks," . *Computers & Security* , vol. 24, pp. 31-43, 2005..

[7] K, R. (2011, March 15). Retrieved from http://www.excitingip.com/1500/an-introduction-to-ddos-distributed-denial-of-service-attack.

[8] Kiruthika Devi, B. S., & Subbulakshmi, T. (2016). A Comparative Analysis of Security Methods for DDoS Attacks in the Cloud Computing Environment. *Indian Journal of Science and Technology* .

[9] Mishra, A., Gupta, B. B., & Joshi, R. C. (2011). "A Comparative study of Distributed Denial of Service Attacks, Intrusion Tolerance and mitigation Techniques". *European Intelligence and Security Informatics Conference* (pp. 286-289). IEEE Computer Society.

[10] Patani, N., & Patel, R. (2017). "A Mechanism for prevention of flooding based DDoS Attack". *International Journal of Computational Intelligence Research* .

[11] Rajkumar, P., & Selvakumar, S. (2011). "Distributed denial of service attack detection using an ensemble of neural classifier". *Computer Communications* , *34*, 1328-1341.

[12] Reddy, M. R., & Yalla, P. (March-2016). "Mathematical Analysis of Penetration Testing and Vulnerability Countermeasures". *2nd IEEE International Conference on Engineering and Technology.* Coimbatore, TN, India.: IEEE.

[13] Shanley, A., & M.J. (2015). "Selection of Penetration Testing Methodoligies: A Comparison and Evaluation". *Australian Information Security Management Conference.*

[14] Shaukat, K., Faisal, A., Masood, R., Usman, A., & Shaukat, U. (2016). *"Security Quality Assurance through Penetration Testing"*. IEEE.

[15] Shivayogimath, C. N. (July-2014). "An Overview of Network Penetration Testing". *International Journal of Research in Engineering and Technology , 3* (7), 408-413.

[16] Shubh, T., & Sharma, S. (2016). "Man-In-The-Middle Attack Prevention Using HTTPS and SSL". *International Journal of Computer Science and Mobile Computing* , 569-579.

[17] singh, H., Jangra, S., & Verma, P. K. (May-2016). "Penetration Testing:Analyzing the Security of the Network by Hacker's Mind". *International Journal of Latest Technology in Engineering, Management and Applied Science , V* (V), 56-60.

[18] Specht, S. M., & Lee, R. B. (September2004). " Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures.". *17th International Conference on Parallel and Distributed Computing Systems*, (pp. 543-550).

[19] Sudhodanan, A., Carbone, R., Compagna, L., Dolgin, N., Armando, A., & Morelli, U. (2017). "Large-scale Analysis & Detection of Authentication Cross-site Request Forgeries". *IEEE European Symposium on Security and Privacy*, (pp. 350-365).

[20] *Symantec Security Report.* (April 2017) https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf.

[21] Yadav, R. K. (2015). " MAN IN MIDDLE ATTACK IN SSL AND HTTPS". *International Journal of Computer Science and Mobile Computing* .