ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 2, Issue 3, March 2016

Improved Technique Survey of Security Attacks in Information-Centric Networking

[1]Ajin .A, [2]Mr.G.Ashwin, [3]Dr.A.Lenin Fred.

[1]PG Scholar, [2]Assistant Professor, [3]Professor, Computer Science & Engineering,
Mar Ephraem College of Engineering & Technology,
Elavuvilai, Marthandam, India

***Abstract*— This proposes ICN focuses on content retrieval from the network regardless of storage location or physical representation of this content. It provide a survey of attacks unique to ICN architectures and other generic attacks that have an impact on ICN. It classified into four main categories: naming, routing, caching, and other miscellaneous related attacks. It shows the relation between ICN attacks and unique ICN attributes; ICN attacks and security requirements: confidentiality, integrity, availability, and privacy.**

***Index Terms*— ICN, Confidentiality, Integrity, Security Requirements**

I. INTRODUCTION

A. *Network Security*

ICN architectures focus on contents or information objects and their properties in the network. ICN is also concerned about receiver interests. In order to achieve these goals, ICN relies on location independent naming, in network caching, and name-based routing. In ICN, senders do not send content directly to receivers. A sender publishes advertisement messages to tell the network that it has some content to share, without necessarily knowing who may be interested in it. On the other side, a receiver declares its interest for some content, not necessarily knowing the senders who have published this content. The ICN network makes a delivery path from the sender to the receiver when there is a match between sender's publication and receiver's subscription. Finally, the content is transferred to the receiver.

B. *Scope of the project*

Survey of attacks unique to ICN architectures and other generic attacks that have an impact on ICN. It also provides taxonomy of these attacks in ICN, which are classified into four main categories: naming, routing, caching, and other miscellaneous related attacks. Shows the relation between ICN attacks and unique ICN attributes.

C. *Networking Basics*

In addition to switches, networks generally employ routers as well. These essential tools connect different networks to each other through the internet in order to allow for data exchange between networks. Whereas the switch can be considered a controller, a router should be considered more of a dispatcher, packaging digital information and choosing the best route for it to travel. Routers can feature several other functions, including firewalls and virtual private networks (VPNs) that enhance the security of the data being sent over the internet.

D. *Network Types*

There are countless types of networks available, especially as networking technologies continue to advance. Two of the most commonly employed networks are LAN and WAN.

E. *Local Area Network (LAN):*

These networks are used to connect devices over relatively short distances, such as within a building, school, or home. LANs generally employ Ethernet cables as a means of connecting the various gadgets within the network.

• Wide Area Network (WAN): These networks are used to connect devices over much larger distances than LANs. A WAN is established by using routers to connect various LANs and is generally not owned by a single person or organization. The internet is one massive WAN that spans the entire planet.

• Other Network Types: Various other types of networks exist, including wireless local area networks (WLANs) that are LANs based on wireless network technology and metropolitan area networks (MANs) that cover larger areas than LANs but smaller areas than WANs. These MANs generally span a city and are owned and operated by a government or corporation.

F. *Network Topology*

Not to be confused with network type, network topology refers to the virtual layout of the devices within a network and

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 2, Issue 3, March 2016

can refer to five distinct categories:

• Bus: This topology utilizes a common backbone, generally a single cable, to connect all the devices on a network.
• Ring: Found in some offices and schools, ring topologies give each device two neighbors for communication purposes. All data travels in a ring, and a failure of that ring can bring down the whole network.
• Star: Found in many homes, a central connection known as a "hub" is connected to all the objects on the network. This hub could be a router or a switch.
• Tree: A hybrid bus/star network, several star hubs are connected to the core cable of a bus in order to vastly increase the number of computers able to connect to the network.
• Mesh: The mesh topology employs the concept of routing, in which each piece of data sent on the network has multiple paths it can take instead of one fixed route. The internet is a perfect example of this topology.

G. *Computer Network Definition*

A computer network is a collection of computers and other devices that are able to communicate with each other and share data. These devices include computers, printers, tablets, phones, and many other electronics.

H. *Computer Networking Essentials*

Both traditional and modern forms of computer networking aim to provide users with the ability to share data amongst multiple gadgets, whether they be in the same building or across the globe. Traditional computer networking relied on Ethernet and fiber optic cables to connect various devices on a network. More modern technology has emerged that allows for wireless connections between electronics. These technologies include Wi-Fi and Bluetooth compatible devices. It is very helpful to understand the role that each of these technologies plays in computer networking.

• **Wide Area Interconnects:** Networks that must support large volumes of devices simultaneously, such as satellites or cellular networks are considered wide area interconnects. They are generally expensive to build and run more slowly than others due to the large area and high volume of users.
• **Long Distance Interconnects:** These include cables such as Ethernet and fiber optics. They support a very large amount of data and serve many clients who share common hardware.
• **Short Distance Interconnects:** These technologies are much newer than other the others and include tools such as Bluetooth. These interconnects are highly optimized for low-cost and also low power usage. Bluetooth is used in many mobile devices, laptop computers, and speakers in order to enable the transfer of data. Popular information sent over Bluetooth includes music, phone calls, and contact information. The market for Bluetooth technology is growing at a rapid pace to include many other items such as remote controlled helicopters and cars, home security systems, and fitness gear. Because it is rather affordable for the connectivity it supplies, Bluetooth technology is finding its way into countless niches.

I. *Computer Networking*

- **The Server**

In information technology, a server is considered any instance of an application that can receive and serve the requests of other programs. Usually these applications are run on computers dedicated to acting solely as servers so that the heavy burden of fulfilling requests from other devices on the network does not overwhelm the computers. Running servers on dedicated computers is also a safety measure, helping to keep the server from being attacked. The computers dedicated to acting as servers usually include faster CPUs, bigger hard drives, better RAM, and multiple power sources. These enhancements allow the server to handle the immense workload and also give it reliability in the event of unfortunate events.

J. *Peer – To - Peer Networks*

A Peer-to-Peer network, or P2P network, is one in which multiple computers are connected without linking through a separate computer that acts as a server. These connections can vary based on how many computers are being linked together. Two computers can be linked via a USB drive to allow for the transfer of files. In [15], *Christo Ananth et al.* discussed in which The analytical model can capture the details of WiMAX resource allocation and take into consideration the popularity of the mobile Television contents being viewed by users enabling it to provide an accurate estimate of the amount of bandwidth required for WiMAX TV services and also enabling a designer to optimally select the number of channels via the WSDV service while meeting a desired level of blocking probability. Multiple computers in an office can be connected directly to each other via traditional copper wiring instead of through a server computer. The fundamental basis for P2P networks is that individual permissions must be set for each computer on the network. For instance, if one computer (A) is connected to a printer and another computer (B) on the network wishes to use the printer, then A would first have to grant B permission.

K. *Network Security*

Network Security is an organization's strategy and provisions for ensuring the security of its assets and of all network traffic. Network security is manifested in an implementation of security policy, hardware, and software. For the purposes of this discussion, the following approach is adopted in an effort to view network security in its entirety:

- Policy

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 2, Issue 3, March 2016

- Enforcement
- Auditing
- Policy

The IT Security Policy is the principle document for network security. Its goal is to outline the rules for ensuring the security of organizational assets. Employees today utilize several tools and applications to conduct business productively. Policy that is driven from the organization's culture supports these routines and focuses on the safe enablement of these tools to its employees. The enforcement and auditing procedures for any regulatory compliance an organization is required to meet must be mapped out in the policy as well.

L. *Enforcement*

Most definitions of network security are narrowed to the enforcement mechanism. Enforcement concerns analyzing all network traffic flows and should aim to preserve the confidentiality, integrity, and availability of all systems and information on the network. These three principles compose the CIA triad:

Confidentiality - involves the protection of assets from unauthorized entities

Integrity - ensuring the modification of assets is handled in a specified and authorized manner

Availability - a state of the system in which authorized users have continuous access to said assets. Strong enforcement strives to provide CIA to network traffic flows. This begins with a classification of traffic flows by application, user, and content. In [11], *Christo Ananth et al.* discussed in which FAQ-MAST TCP aims to rapidly stabilize high-speed long-latency networks into steady, efficient and fair operating points, in dynamic sharing environments, and the preliminary results are produced as output of our project. The Proposed architecture is explained with the help of an existing real-time example as to explain why FAQ-MAST TCP download is chosen rather than FTP download. As the vehicle for content, all applications must first be identified by the firewall regardless of port, protocol, evasive tactic, or SSL. Proper application identification allows for full visibility of the content it carries. Policy management can be simplified by identifying applications and mapping their use to a user identity while inspecting the content at all times for the preservation of CIA.

The concept of defense in depth is observed as a best practice in network security, prescribing for the network to be secured in layers. These layers apply an assortment of security controls to sift out threats trying to enter the network:

- Access control
- Identification
- Authentication
- Malware detection
- Encryption
- File type filtering
- URL filtering
- Content filtering

These layers are built through the deployment of firewalls, intrusion prevention systems (IPS), and antivirus components. Among the components for enforcement, the firewall (an access control mechanism) is the foundation of network security.

M. *Auditing*

The auditing process of network security requires checking back on enforcement measures to determine how well they have aligned with the security policy. Auditing encourages continuous improvement by requiring organizations to reflect on the implementation of their policy on a consistent basis. This gives organizations the opportunity to adjust their policy and enforcement strategy in areas of evolving need.

N. *Problem Statement*

It is crucial to have a comprehensive understanding of the ICN attacks. Existing solutions target a specific architecture or specific types of attacks.

O. *System Requirements*

HARDWARE		**SOFTWARE**	
Processor	Pentium IV 2.6GHz,Intel Core 2 Duo	Front End	JAVA (j2ee, Servlets, jsp)
RAM	512 MB DD-RAM	Back End	MY SQL 5.5
MONITOR	15'' Color	Operating System	Windows 7
Hard Disk	40GB	IDE	Eclipse

II. SYSTEM DESIGN

A. *Proposed System Model*

Proposed Concept

- Survey of attacks unique to ICN architectures and other generic attacks that have an impact on ICN.
- It also provides taxonomy of these attacks in ICN which are classified into four main categories: naming, routing, caching and other miscellaneous related attacks.
- Shows the relation between ICN attacks and unique ICN attributes.

Advantages of Proposed System

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 2, Issue 3, March 2016

- Develop taxonomy of ICN attacks and classify the attacks into four categories: naming, routing, caching, and other miscellaneous related attacks.
- Shows the relation between ICN attacks and unique ICN attributes

Proposed System Enrichment

- New attacks in ICN environments. These include bogus announcements and time analysis attacks.
- Attacks that occur in both non-ICN and ICN environments in the same way but with a different impact

B. Proposed Algorithm

i. Ranking Algorithm

Ranking algorithm based on the consumer feedback, which allows routers to distinguish between valid and malicious contents. Also there are many works for cache poisoning attacks as in the Domain Name System Security Extensions and the security solution for thwarting cache poisoning attacks in the DNS hierarchy.

1. Regs ← load(name);
2. If register received then
3. If duplicate or invalid signature then
4. Return;
5. End
6. Set. timer_ for_ expiration(register);
7. Else
8. // A REGISTER expired,,,,,,
9. End
10. For each out in provider and peer links do
11. Pref_ reg ← decision. process(out, regs);
12. If pref_ reg changed for out there
13. Msg ← new_ message(pref_ reg);
14. Add_ intra_ cost(out, msg);
15. Sign_ message(private_ key, msg);
16. Queue(out, msg);
17. End
18. End
19. Store(name, all changes);

System Architecture

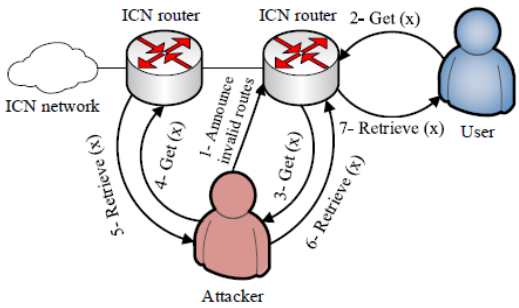


Figure 2 Architecture 1

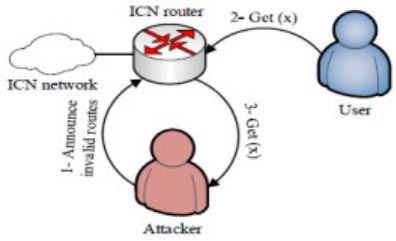


Figure 3 Architecture 2

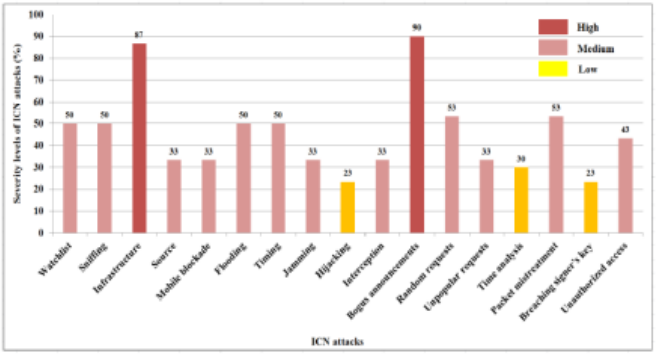


Fig 1: Security levels of ICN attacks

C. System Architecture Explanation

Ranking algorithm based on the consumer feedback, which allows routers to distinguish between valid and malicious contents. Also there are many works for cache poisoning attacks as in the Domain Name System Security and the security solution for thwarting cache poisoning attacks in the DNS hierarchy.

D. Modules

- User Interface Design
- Sender Publishing Advertisement Message
- Receiver Requesting for Advertisement
- Attackers
- Survey of the Attacks

E. Module Description

a. User Interface Design

This is the first module of our project. The important role for the Network user is to move login window to cloud user window. This module has created for the security purpose. In this login page we have to enter login user id and password. It will check username and password is match or not (valid user name and valid password).

If we enter any invalid username or password we can't enter into login window to user window it will shows error message. So we are preventing from unauthorized user entering into the login window to user window. It will provide a good security for our project. So server contain user id and password server also check the authentication of the user.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 2, Issue 3, March 2016

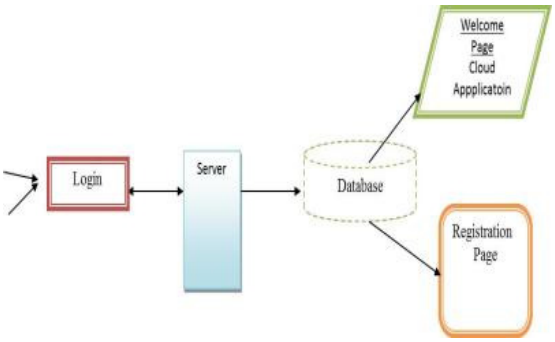


Fig 4: User Interface Design

b. Sender Publishing Advertisement Message

In this module A sender publishes advertisement messages to tell the network that it has some content to share, without necessarily knowing who may be interested in it. Sender publish its advertisement message on behalf of himself he can able to modify the Ad message and Change the content of Message. He/she can able to send response message to the user he/she interested or he can able omits the users by saying that he/she has not interested on the User.

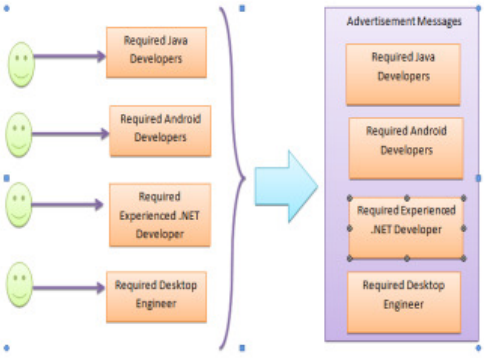


Fig 5: Sender Publishing Advertisement Message

c. Receiver Requesting for Advertisement

On the other side, a receiver declares its interest for some content, not necessarily knowing the senders who have published this content. Receiver even he/she send their response to the Message that Server sends there is no way of declaring that the message from receiver will surely send to the Server. Before that message receiving to serve the file may be attacked by the Unknown Attackers. Next Modules show how attacks happen and how to overcome it.

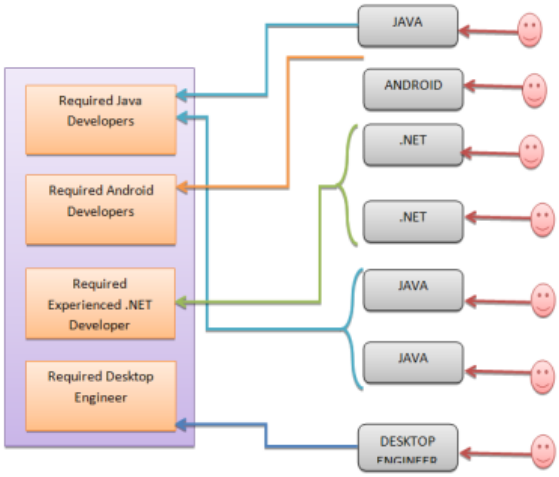


Fig 6: Receiver Requesting for Advertisement

d. Attackers

In this module the user itself act as attackers with the list of available attacks they can produce. If they want data to retrieve in normal mode they can retrieve it if user want any attack want to happen to that file they can choose which attack need to happen. Network Attacks namely naming, routing, cache, other miscellaneous attacks that may cause harm to your files. Naming Attack i.e., the Attacker may delete the request that the user send to server. Routing Attack i.e., the Attacker may change the path of the receiver. Cache Attacks i.e., the Attacker make a unwanted updates so that it causes to work load. Finally Miscellaneous Attacks ie., the Attacks happens during downloading time user may not able to download the file he/she wants.

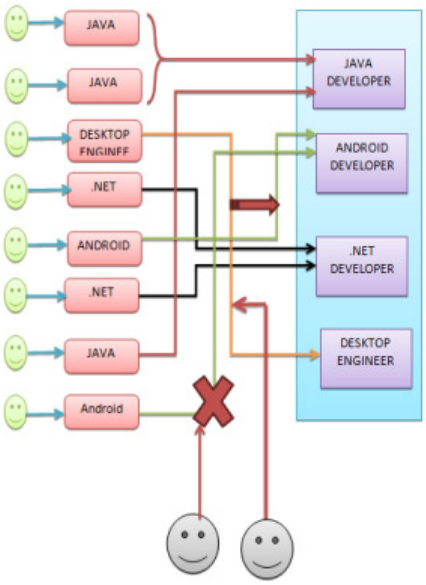


Fig 7: Attackers

e. Survey of the Attacks

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 2, Issue 3, March 2016

This module shows that what type of attack happens to your file and how much security is given to it. A alert or graphical representation will be shown to the user on the types of attacks that are happens to the file and how much security is given to the file. If we secured our files from those attacks a message will be shown to the user your file has been Secured from this Network attacks.

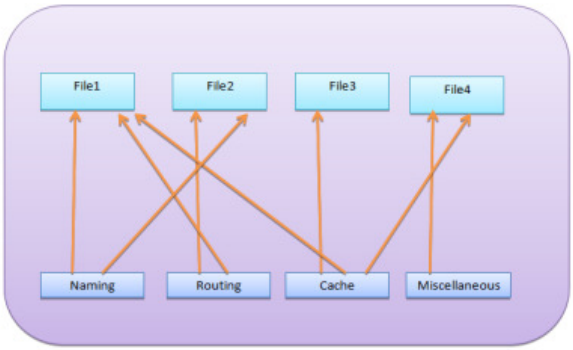


Fig 8: Survey of the Attacks

F. Input Expected Output

- User Interface Design

Input : User Login name and Password
Output : If Valid user Open the user window otherwise error page.

- Sender Publishing Advertisement Message

Input : Sender Sends the Advertisement Message For receiver .
Output : He can Monitor Her advertisement based on Receiver Request.

- Receiver Requesting for Advertisement

Input : Advertisement Message
Output: Sending Interest based on Advertisement

- Attackers

Input : Types of Attacks
Output : How each attacks make Change to the Advertisement

- Survey of Attacks

Input : Advertisement Message.
Output: Types of Attacks that attack the File

III. RESULT & ANALYSIS

A. Registration

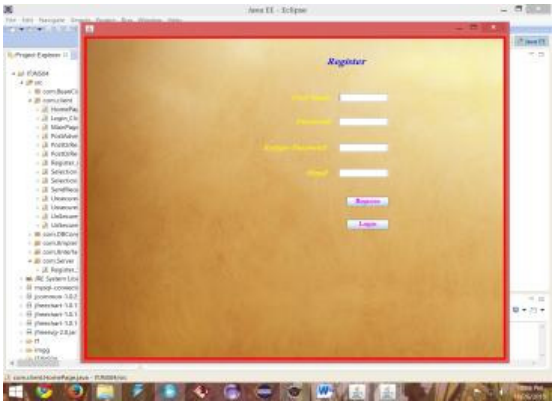


Fig 9: Registration Page

The models of registration forms are as follows:-

The figure below shows the registration process is completed successfully.

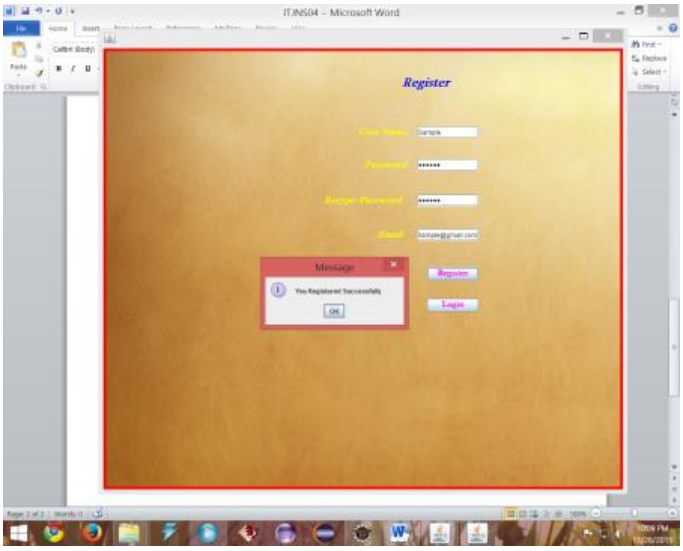
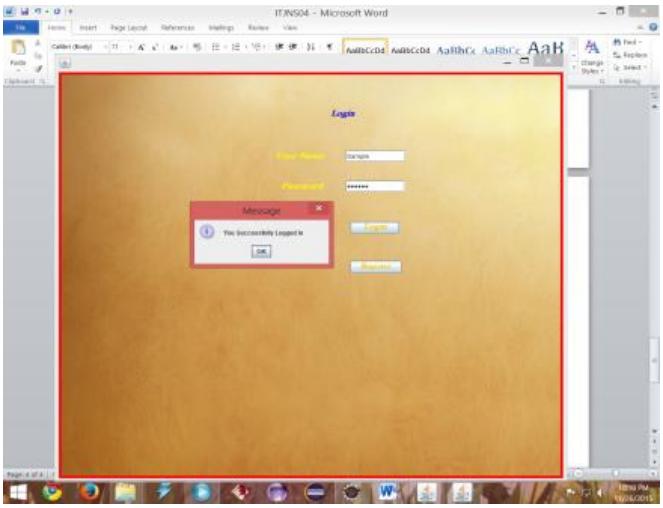


Fig 10: Registered Successfully Page



ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 2, Issue 3, March 2016

Fig 11: Login Page

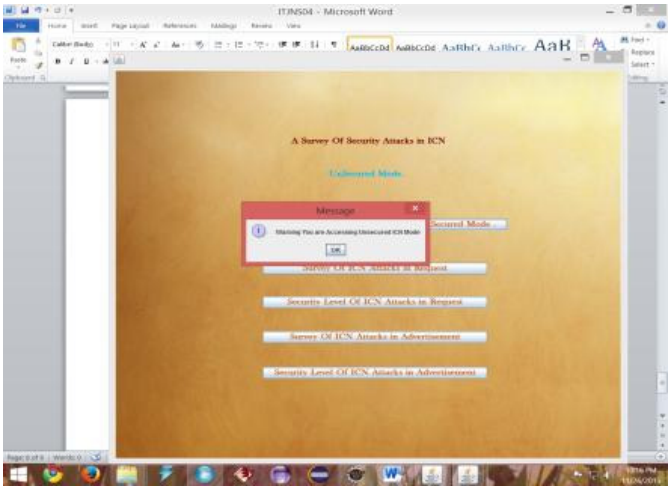


Figure: 12 Security alert

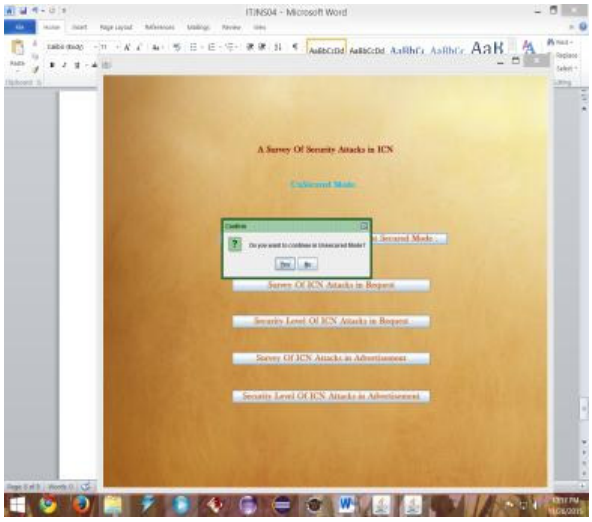


Figure13: Conformation Tab

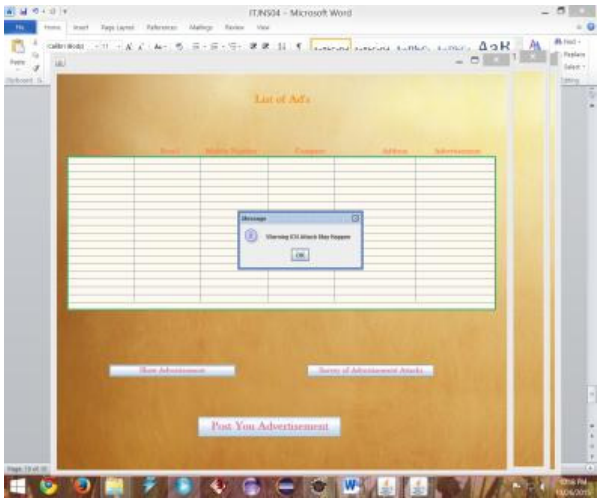


Figure: 14 Advertisement Posting

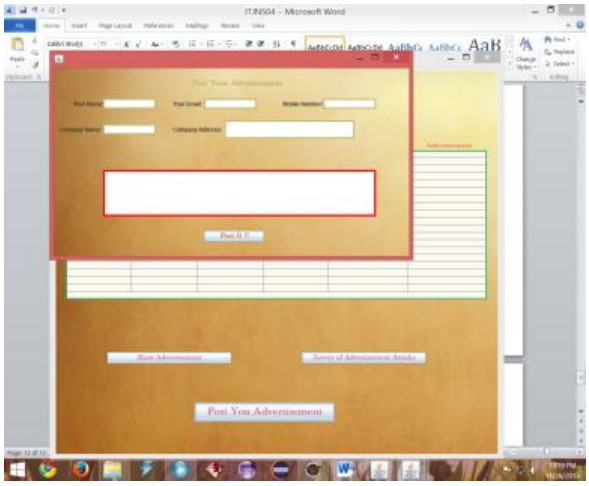


Figure: 15 Advertisement Details

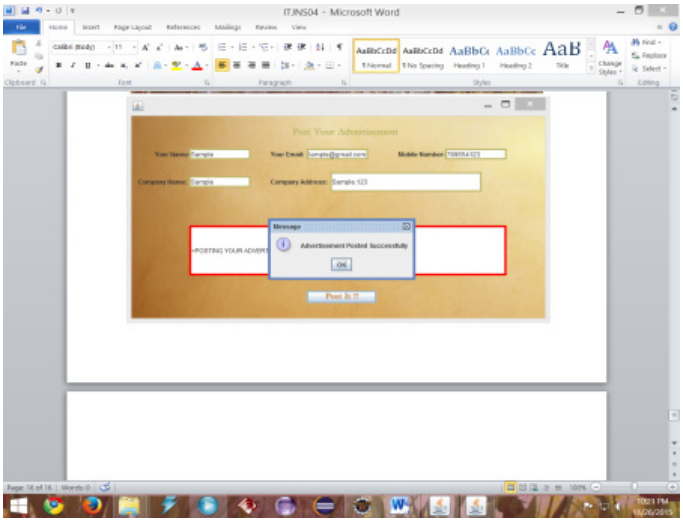


Figure 16 Conformation tab

IV. Conclusion And Future Scope

A. *Conclusion*

ICN, as one of these solutions focuses on contents to provide a scalable and efficient content delivery. There are many proposals for ICN architectures like DONA, NetInf, NDN, and PURSUIT. ICN has attributes that make it unique from host-centric architectures. ICN mainly depends on location independent naming, in-network caching, and name-based routing. The future internet comes with high requirements of information dissemination, which motivate the research community to find alternative solutions. ICN, as one of these solutions focuses on contents to provide a scalable and efficient content delivery. ICN has attributes that make it unique from host-centric architectures. ICN mainly depends on location independent naming, in-network caching, and name-based routing

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE)
Vol. 2, Issue 3, March 2016

B. *Future Enhancement*

The future internet comes with high requirements of information dissemination, which motivate the research community to find alternative solutions. ICN, as one of these solutions focuses on contents to provide a scalable and efficient content delivery.

REFERENCES

[1] "Cisco visual networking index: forecast and methodology", 2012-2017, May 29,2013.

[2] H. Moustafa and S. Zeadally, "Media networks: architectures, applications and standards", CRC Press, 2012.

[3] J. Pan, S. Paul, and R. Jain, "A survey of the research on future internet architectures", IEEE Communications Magazine, vol. 49, no. 7, July 2011, pp. 26 36.

[4] M. K. Pathan and B. Rajkumar, "A taxonomy and survey of content delivery networks", Grid Computing and Distributed Systems Laboratory, University of Melbourne, Technical Report, 2007.

[5] E. Lua, J. Crowcroft, M. Pias, R. Sharma, and S. Lim, "A survey and n comparison of peer-to-peer overlay network schemes", IEEE Communications Surveys & Tutorials, vol. 7, no. 2, pp. 72-93, 2005.

[6] D. Cheriton and M. Gritter, "TRIAD:A scalable deployable NAT based Internet architecture", Technical Report, January 2000. [Online]. Available: http://ceng.anadolu.edu.tr/cakinlar/BIL555/icerik/2000,Triad.pdf, accessed on 6 June 2014.

[7] T. Koponen, M. Chawla, B. G. Chun, A. Ermolinskiy, K. H. Kim,S. Shenker and I. Stoica, "A data-oriented (and beyond) network architecture", SIGCOMM Comput. Commun. Rev., vol. 37, no. 4, 2007, pp. 181- 192.

[8] "The network of information: architecture and applications", FP7-ICT-2009-5-257448-SAIL/D-3.1, July 2011, [Online]. Available: http://www.sail-project.eu/wp-content/uploads/2011/08/SAIL DB1 v1 0 final-Public.pdf, accessed on 6 June 2014.

[9] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, and R. Braynard, "Networking named content", CoNEXT'09, ACM, December 2009, pp. 1-12.

[10] D. Lagutin, K. Visala, and S. Tarkoma, "Publish/subscribe for internet: PSIRP perspective", Towards the Future Internet, IOS Press, vol. 4, 2010, pp. 75-84.

[11] Christo Ananth, S.Esakki Rajavel, I.AnnaDurai, A.Mydeen@SyedAli, C.Sudalai@UtchiMahali, M.Ruban Kingston, "FAQ-MAST TCP for Secure Download", International Journal of Communication and Computer Technologies (IJCCTS), Volume 02 – No.13 Issue: 01 , Mar 2014, pp 78-85

[12] Md. F. Bari, S. R. Chowdhury, R. Ahmed, R. Boutaba, and B. Mathieu, "A survey of naming and routing in information-centric networks", IEEE Communications Magazine, vol. 49, no. 12, December 2012, pp. 44-53

[13] C. Tsilopoulos, X. Vasilakos, K. Katsaros, G. Polyzos, G. Xylomenos, C. Ververidis, V. Siris, and N. Fotiou, "A survey of information-centricnetworking research", IEEE Communications Surveys & Tutorials, July 2013.

[14] C. Dannewitz, J. Golic, B. Ohlman, and B. Ahlgren, "Secure naming for a network of information", in Proc. of the IEEE Infocom, March 2010, pp. 1

[15] Christo Ananth, M. Suresh Chinnathampy, S. Allwin Devaraj, S. Esakki Rajavel, V. Kulandai Selvan, P. Kannan, "CAPACITY BEHAVIOUR USING WSDV SCHEME OVER WIMAX", ABHIYANTRIKI-An International Journal of Engineering & Technology (AIJET), Vol. 1, No. 2,December 2014,pp:18-27

[16] Ghodsi, T. Koponen, B. Raghavan, S. Shenker, A. Singla, and J. Wilcox, "Information-centric networking: seeing the forest for the trees", in Proc. of the 10th ACM Workshop on Hot Topics in Networks, ACM,2011, pp. 1-6.

[17] F. Almeida and J. Loureno, "Information centric networks-design issues, principles and approaches", International Journal of Latest Trends in Computing, vol. 3, no. 3, September 2012, pp. 58-66.

[18] D. Djenouri, L. Khelladi, and A. Badache, "A survey of security issues in mobile ad hoc and sensor networks", IEEE Communications Surveys & Tutorials, vol. 7, no. 4, 2005, pp. 2-28.

AUTHORS BIOGRAPHY

A.Ajin was born on 29th November 1988. He attended an International Seminar at Agni college of Engineering & technology,Chennai on Digital Image Processing and its applications.. He has also attended an Industry Oriented training camp on GNU/LINUX organized by free software movement,wipro at SSN College of Engineering Chennai. He has attended an International Conference on Trends in Computational Engineering and Technology at Tamizhan College of Engineering & Technology, Nagercoil.Currently He is a PG Scholar at Mar Ephraem College of Engineering and Technology in the department of computer science and engineering. He had completed his UG at Hindustan College of Engineering,Chennai. in the department of Information Technology. His area of interest is working on Network Security.