RESEARCH ARTICLE OPEN ACCESS

A STUDY OF WI-FI ACCESS DATA SECURITY IN INTERNET OF THINGS

M.Balamurugan*,Dr.R.Kalaiarasi**

*Assistant Professor, Department of BCA, Immaculate College for Women, Viriyur.
** Assistant Professor, School of Computer Science, Tamil nadu Open University, Chennai-15.

ABSTRACT:

This paper proposed to strong process data generated from the Internet of Things moreover has a great impact on data protection support as wi-fi technology . data protection is potentially still more critical than predictable data. The challenges to bring huge data storage also impact data security particularly when dealing with sensor data, all most backing applications don't handle billions of files as well. Humans are fast being outnumbered by Internet-connected devices that are continuously collecting and transmitting data is used to term as the Internet of Things. And one more proposed IOT support large amount of date accessing through wifi and other process still (i.e) mobile shop, shopping mall , public access places enclosed process free access that expensive about large level that get for another idea for control access process iot technology then wifi technology two structure one for authentication another for password lock but some public places open process access example a big mobile shop. Any other buyer still access to new mobile access .still through other neighbors they can also access to own process and wifi frequency level broad brand that outdoor public people they most access to wifi process that problem occurred to shop owners but we are implement that new idea when your purchase new arrival mobile model that time mobile ip address and checking access security code allocate wifi technology not access password process only the mobile address allocate specify address access to pair process another mobile does not have automatically disconnect so I would like to implement that source IOT process .

Keyword: IOT,wifi, mobile ip.

1.INTRODUCTION

The Internet of Things is becoming very important topic in technology business, policy, and engineering circles and has become headline news in each of the specialty press and media. This technology is embodied during a wide spectrum of networked merchandise, systems, security and sensors that make the most of advancements in computing power, natural philosophy miniaturization, and network interconnections to supply new capabilities not antecedently potential. Associate degree abundance of conferences, reports, and news articles discuss the possible impact of the "IOT revolution" from new market opportunities and business models to considerations concerning security, privacy, and technical ability. IOT web society community navigate the dialogue close to the web of things in lightweight of the competitor predictions concern is guaranteed. It provides a high level review of the fundamentals of IOT and a few of the key problems and queries that this technology raises from the attitude tend to be the internet of things. WiFi is surrounding us. What technologies will define future WiFi ? Will key technologies related to WiFi creates road map towards its future or emerging super WiFi technologies extends? This paper focuses on new development alternatives that creates wireless access solutions means future of WiFi.

2.ISSUES AND CHALLENGES

The number of connected devices increases and their usage becomes an important part of everyday life. Security, Privacy and Personal safety issues were

need of the hour. Security issues are already seen to inhibit the uptake of cloud services, particularly by public bodies with responsibility for sensitive information, reminiscent of attention services. Because the variety of sources/sinks will increase, managing and securing these suitably becomes a challenge. Privacy is also an important challenge to keep the personal information which is collected must be safely guarded and secured source of information need to be properly handled.

3. ACCESS IDEA:

3.1. Motivation of IoT:

Focus on security concerns for IOT from the views of cloud tenants, end-users and cloud suppliers, within the context of wide-scale IOT proliferation, operating across the vary of IOT technologies.

3.2. Security on internet wifi acces:

A cooperative approach to security are required to develop an effective and applicable solutions to IOT security challenges that are similar temperament to the dimensions and complexness of the problems. While security concerns aren't new within the context of knowledge technology, the attributes of the many IOT implementations gift new and distinctive security challenges. Addressing these challenges and guaranteeing security in IOT merchandise and services should be a elementary priority. User have to be compelled to trust that IOT devices and connect knowledge services are secure from vulnerabilities, particularly as this technology become an additional pervasive and integrated into our daily lives. Poorly secured IOT devices and services will function potential entry points for cyber attack and expose user knowledge to thieving by exploit knowledge streams inadequately protected.

3.3.Advanced Enterprise Wifi

The new wireless technologies for enterprise environments in 2014 will change the trends of enterprise employees. The different ways will advance in coming years such as:

• Adoption of 802.11ad which represents the upcoming change in the IEEE 802.11 protocol and increases the data speed into the Gigabit world.

• Expansion of cloud for small and medium sized enterprises.

• WiFi- based location analytics will help for differ ent organization to improve the customers and user WiFi experience, to increase bus iness intelligence and to improving the security policy.

• BY using advance Hot Spot 2.0 and pass point open s ervices.

• To allow user to log in to the WiFi network by using their social credentials.

Our homes have become complex networking environments with numerous devices utilizing the wireless spectrum in countless ways. In addition to the streaming and gaming applications which have become common-place, today's homes are increasingly becoming filled with a growing number of devices such as cameras, health and motion sensors, thermostats, etc. Unless a home is located in the "middle of nowhere," it is more than likely that neighboring home Wi-Fi networks will "step on each other's feet", i.e. , associated network flows from different networks will interfere with each other, heavily affecting performance.

Wi Fi has proved to be immensely popular with smartphone users as a low cost solution for improved localised coverage and mobile broadband experience, at venue specific locations especially indoors. I ndustry sources state that between 60 % or

80% of traffic on a smartphone today is carried over Wi - Fi

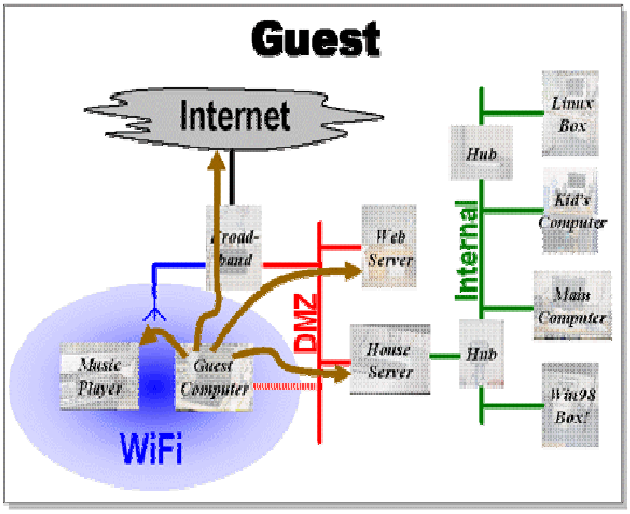
1 . What is less evident is the extent to which Wi Fi can provide capacity relief to the cellular networks, either from existing Wi - Fi networks or potentially from new implementations such as small cells. With such high traffic volumes on Wi - Fi, it would be easy to infer that a high proportion of traffic is being offloaded from the cellular networks

2 , reducing the need for additional cellular spectrum. But is this view valid? This paper examines this question from a number of perspectives. Is traffic carried over Wi - Fi incremental or replacement?

2. Do today's coverage led Wi - Fi networks reduce cellular traffic load where it matters?

3. How suitable is Wi - Fi as the base technology for small cell solution for cellular capacity expansion?

4. What is the business motivation model for Wi - fi networks to be built for cellular capacity relief?



4. NETWORK PLANNING IN MOBILE ACCESS PASSWORD

For any rural system, cost is the primary consideration in every step of the design. Next to the choice of technology

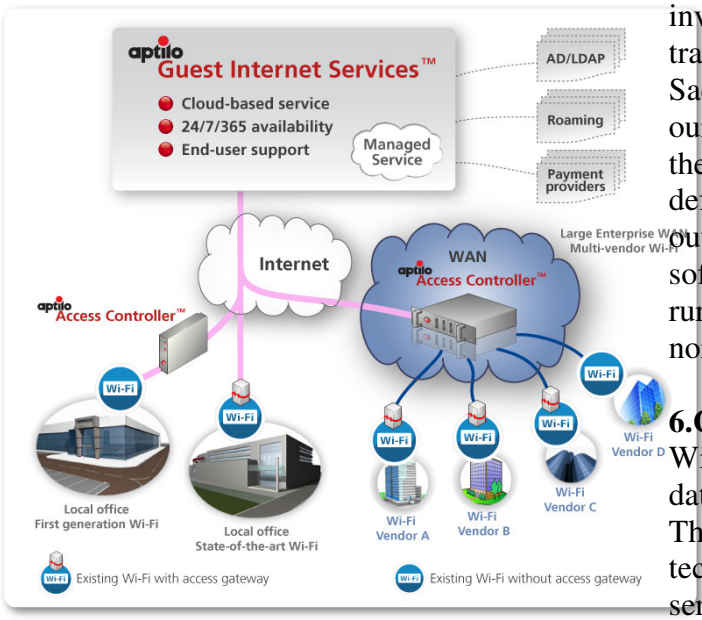
(WiFi), the context in which cost optimization is significant is in network planning and ip address setting .

We elaborate on this issue below. A long-distance WiFi link requires line-of-sight to get sufficient signal strength for reception; otherwise the attenuation in 2.4 GHz or 5 GHz is too high beyond a few hundred meters. This in turn implies that network deployment involves significant infrastructure in terms of antenna towers. The a p-proximate cost of antenna towers/masts is In comparison, note that WiFi radio cost can be about $50 or less. Tall towers are one or two orders of magnitude costlier than the radio equipment! Hence in long-distance WiFi deployments, network plan- . Typical antenna tower/mast costing to optimize the infrastructure cost will play a significant role. This is quite unlike WiFi-based community networks in metropolitan areas where an adhoc deployment model is workable. Apart from cost reduction, a secondary concern requiring network planning in our setting is to guarantee a minimum level of performance to each village node. A simple way to quantify this performance is in terms of the achievable net- work throughput to each village while operating at capacity . For instance, in the Ashwini project, we have a requirement of providing at least 384 Kbps to each village to enable high- quality video-conferencing.

Network planning considering cost and performance involves at least six related aspects: (1) the tower locations

, representing the nodes of the network, (2) tower heights at each location, (3) what links to form, to have a connected network topology, (4) what antenna types to use for

each link, (5) the transmit powers to use for each radio, and (6) the channel of operation for each link. Typically, the broad locations of the towers are chosen to be the villages where network connectivity is desired. Further, the finer choice of where in each village to locate the towers is also typically done based on non-technical reasons of convenience of operation. This has been the case both in DGP as well as In general however, a commercial deployment may choose its towers to be located at places where the height above MSL (Mean Sea Level) is higher in comparison to the others. This is to help reduce the tower height requirement.



5.NETWORK MANAGEMENT AND ISSUES IOT ACCESS:

Network management consists of performance and fault diagnosis and repair. It is known that such management is more complicated in wireless networks in comparison with traditional wired networks. There are far more reasons for bad behaviour of wireless performance: interference from other WiFi sources, from other non-WiFi sources, signal strength variation, etc. While work is in progress to address network management in enterprise WiFi networks (e.g. 802.11v, 802.11k), this Is not the case for long-distance settings. The remote diagnos is and repair of these problems is especially important to address in long-distance WiFi networks for several reasons: (1) any physical visit required would involve significant cost since the distances involved are large, (2) rural locations are relatively inaccessible, and (3) the availability of trained personnel in rural areas is relatively poor. To present an extreme case, visiting the Sarauhan site of the DGP test bed to diagnose any problem involves close to an entire working day of travel (6 hours) of 1-2 trained personnel . Sadly, one of the prime reasons requiring our visit there has been a simple problem: the WiFi bridge resets its settings to factory defaults if it is rebooted due to a power outage. Clearly, the bridge management software was not designed for operation in rural regions where power outages are the norm rather, than the exception.

6.CONCLUSION

WiFi is unique in that it is an inexpensive data-centric broadband access technology. This makes WiFi a high- potential technology for rural communication services. And implement to IOT wifi control access for un authentication people that process curial happened to in this world There are several technical issues in making WiFi work in long distance rural settings. Despite the radio itself being low cost, the other parts of the system may involve substantial cost and optimization is required to enhance the viability of WiFi. Apart from cost optimization, minimizing power consumption is also an important aspect to

pay attention to in rural settings. Orthogonally, providing the right kind of services package d for rural communities is essential to gain the benefits of information and communication technology.

7. REFERENCES

[1]. Stefan Berger, Kenneth Goldman, Dimitrios Pendarakis, David Safford, Enriquillo Valdez, Mimi Zohar IBM T.J. Watson Research Center Yorktown Heights, New York 10598 "Scalable Attestation: A Step Toward Secure and Trusted Clouds" 2015 IEEE International Conference on Cloud Engineering.

[2].Thomas F. J.-M. Pasquier Julia E. Powles Computer Laboratory, "Expressing and Enforcing Location Requirements in the Cloud using Information Flow Control" 2015 IEEE International Conference on Cloud Engineering.

[3].Ryan K L Ko 1 , Peter Jagadpramana 1 , Miranda Mowbray 2, Siani Pearson 2 , Markus Kirchberg 1 , Qianhui Liang 1 , Bu Sung Lee 1 "TrustCloud: A Framework for Accountability and Trust in Cloud Computing" 2011 IEEE World Congress on Services.

[4].S. Subashini n , V. Kavitha Anna University Tirunelveli, Tirunelveli, TN 627007, India "A survey on security issues in service delivery models of cloud computing" Journal of Network and Computer Applications 34 (2011) 1–11

[5].Pierre de Leusse, Panos Periorellis, Theo Dimitrakos and Srijith K. Nair Newcastle Univeristy British Telecom. "Self Managed Security Cell, a security model for the Internet of Things and Services" 2009 First International Conference on Advances in Future Internet.