Jul - Dec- 2018

TRINITY INSTITUTE OF PROFESSIONAL STUDIES

Dwarka, Sector-9, New Delhi

Trinity Tech Review

Vol 4, Issue 2

Disclaimer: The views and opinions presented in the articles, case studies, research work and other contributions published in Trinity Tech Review (TTR) are solely attributable to the authors of respective contributions. If these are contradictory to any particular person or entity, TTR shall not be liable for the present opinions, inadequacy of the information, any mistakes or inaccuracies.

Trinity Institute of Professional Studies
An ISO 9001:2008 Certified Institution
(Affiliated to Guru Gobind Singh Indraprastha University, Delhi)
Sector-9, Dwarka, New Delhi-110075
Ph: 45636921/22/23/24, Telefax : 45636925
www.tips.edu.in, tips@tips.edu.in

TRINITY INSTITUTE OF PROFESSIONAL STUDIES
Affiliated to Guru Gobind Singh Indraprastha University, Delhi)
"A+" Ranked Institution by SFRC, Govt. of NCT of Delhi.
Recognised under section 2(f) of the UGC Act, 1956
&
NAAC Accredited "B++" Grade Institution

STATEMENT ABOUT OWNERSHIP AND OTHER DETAILS OF TTR/TMR

FORM 5 (RULE 8)

1.	Printer's Name	:	Dr. R.K. Tandon
	Nationality	:	Indian
	Address	:	Trinity Institute of Professional Studies Sector-9, Dwarka, New Delhi 110075
2.	Place of Publication	:	Delhi
3.	Periodicity of Publication	:	Quarterly
4.	Publisher's Name	:	Dr. R.K. Tandon
	Nationality	:	Indian
	Address	:	Trinity Institute of Professional Studies Sector-9, Dwarka, New Delhi 110075
5.	Editor's Name	:	Dr. Vikas Rao Vadi
	Nationality	:	Indian
	Address	:	Trinity Institute of Professional Studies Sector-9, Dwarka, New Delhi 110075
6.	Name and Address of the individual who owns the journal and partners or shareholders holding more than one per cent of the capital.	:	CHAIRMAN Trinity Institute of Professional Studies Sector-9, Dwarka, New Delhi 110075
7.	Hosted at (url)	:	www.tips.edu.in

I, Dr. R.K. Tandon, hereby declare that the particulars given above are true to the best of my knowledge and belief.

Dr. R.K. Tandon

BIG DATA ANALYTICS(HADOOP)

RITIKA KAPOOR
ASSISTANT PROFESSOR, CS & IT DEPT., TIPS DWARKA

ABSTRACT

The Big Data is the most prominent paradigm now-a-days. The promise of data driven decision making is now being recognized broadly, and there is growing enthusiasm for the notion of "Big Data".Big data is a term that describes the large volume of data – both structured and unstructured – that overwhelms a business on a day-to-day basis. But it's not the amount of data that's important. It's what organizations do with the data that matters. Big data can be analyzed for insights that lead to better decisions and strategic business moves. The Big Data started its rule slowly in 2003, and expected to rule and dominate the IT industries at least up to 2030.. The Big Data is blasting everywhere around the World in every domain. The Big Data, a massive amount of data, is able to generate billions of revenue. The secret behind of these billions of revenue is ever growing volume. This paper presents the redefinition of volume of Big Data. The volume is redefined by engaging three other V's, namely, volume, variety, and velocity. 3Vs (volume, variety and velocity) are three defining properties or dimensions of big data. However, the storage and analysis of large amount of high-speed real-time smart building data is a challenging task. There are a number of contemporary Big Data management technologies and advanced analytics techniques that can be used to deal with this challenge. There is a need for an integrated IoT Big Data Analytics (IBDA) framework to fill the research gap in the Big Data Analytics domain. The initial version of the IBDA framework has been developed by using Python and the Big Data Cloud era platform. This paper covers the categorization of big data, its popularity on the web abilities, data available, gains, tools, techniques and applications. One primary conclusion is how Big Data can be dealt effectively and with precision.

Keywords: Volume, Variety, Velocity, IoT big data analytics

INTRODUCTION

In a broad range of application areas, Data is being collected at unprecedented scale. Decisions that were previously based on guesswork or on models of reality can now be based on the data itself. Such Big Data analysis now drives nearly every aspect of our modern society , including mobile services, retail, manufacturing, financial services, life sciences, and physical sciences. The Slogan Digital sky Survey has today become a central resource for astronomers all over the world. The field of Astronomy is being transformed from one where the pictures of the sky was a large part of an astronomers job to one where the pictures are all in a database already and the astronomers task is to find interesting objects and phenomenon in the database. Big Data has the potential to revolutionize not just research but also education.

The sheer size of the data is a major challenge and is the one that can be easily recognized. The analysis of data involves two categories of data - Structured Data and Unstructured Data.

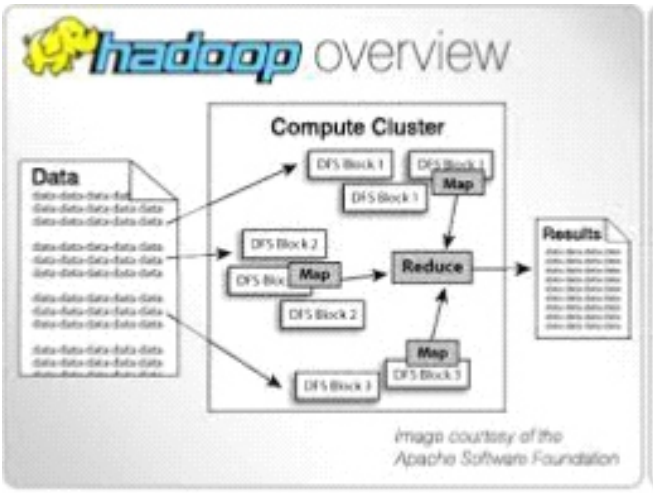
Structured data refers to the data which has a pre-defined data model structure and is often relational in nature and can be easily managed and consumed using the traditional tools/techniques. Unstructured data includes flat files, spread sheets, Word documents, emails, images, audio files, video files, feeds, PDF files, scanned documents, etc.

What is Big Data?

Big data is a buzzword, catch-phrase, used to describe a massive volume of both structured and unstructured data that is so large that it's difficult to process using traditional database and software techniques. Big data helps us to scan and analyse newspaper reports or social media fees so that we can permanently keep speed on the latest developments in industry and environment

- Keeping data safe-

Big data tools allow us to map the entire data landscape across the country. We can
resources. The Hadoop open-source framework uses a simple programming model to enable distributed processing of large data sets on clusters of computers.



The Apache Hadoop Framework
The base Apache Hadoop framework is composed of the following modules:

- Hadoop Common – contains libraries and utilities needed by other Hadoop modules;
- Hadoop YARN – a resource-management platform responsible for managing computing resources in clusters and using them for scheduling of users' applications; and
- HadoopMapReduce –an implementation of the Map Reduce
- Programming model for large scale data processing.

Role of Big Data Hadoop Architect

What does a Big Data Hadoop Architect do?

Typically, a Big Data Hadoop architect addresses specific Big Data problems and requirements. If you take up this role, you will be expected to describe the structure and behavior of a Big Data solution utilizing the Hadoop technology.

You will need to cater to the needs of the organization as well as Big Data specialists and engineers, and act as a link between them. Any organization that wants to build a Big Data environment will require a Big Data architect who can manage the complete life cycle of a Hadoop solution – including requirement analysis, platform selection, design of technical architecture, design of application design and development, testing, and deployment of the proposed solution.

Ensure you meet these primary requirements-

To be a Big Data Hadoop architect, you've got to have advanced data mining and data analytical skills which requires years of professional experience in the Big Data field. If you have the skills listed here, you're on the right track:

- Marketing and analytical skills: The ability to process and analyze data to understand the behavior of the buyer/customer.
- RDMSs (Relational Database Management Systems) or Foundational database skills
- The ability to implement and use NoSQL, Cloud Computing, and Map Reduce
- Skills in statistics and applied math.
- Data visualization and data migration

Moreover, your role as a data architect will be of more importance as many businesses are now turning to data architects than a data analyst or a database engineer.

The Securities Exchange Commission (SEC) is using big data to monitor financial market activity. They are currently using network analytics and natural language processors to catch illegal trading Communications, Media and Entertainment-Since consumers expect rich media on-demand in different formats and in a variety of devices, some big data challenges in the communications, media and entertainment industry include:

1. Collecting, analyzing, and utilizing consumer insights
2. Leveraging mobile and social media content
3. Understanding patterns of real-time, media content usage

Applications of big data in the Communications, media and entertainment industry are:

Organizations in this industry simultaneously analyze customer data along with behaviourial data to create detailed customer profiles that can be used to:

i. Create content for different target audiences
ii. Recommend content on demand
iii. Measure content performance

Spotify, an on-demand music service, uses Hadoop big data analytics, to collect data from its millions of users worldwide and then uses the analyzed data to give informed music recommendations to individual users.
Amazon Prime, which is driven to provide a great customer experience by offering, video, music and Kindle books in a one-stop shop also heavily, utilizes big data.

Big Data Providers in this industry include: Info chimps, Spunk, Pervasive Software, and Visible Measures.

- Healthcare Providers- Industry-Specific challenges are:

The healthcare sector has access to huge amounts of data but has been plagued by failures in utilizing the data to curb the cost of rising healthcare and by inefficient systems that stifle faster and better healthcare benefits across the board.

This is mainly due to the fact that electronic data is unavailable, inadequate, or unusable. Additionally, the healthcare databases that hold health-related information have made it difficult to link data that can show patterns useful in the medical field.

Other challenges related to big data include: the exclusion of patients from the decision making process and the use of data from different readily available sensors.

Applications of big data in the healthcare sector are:

Some hospitals, like Beth Israel, are using data collected from a cell phone app, from millions of patients, to allow doctors to use evidence-based medicine as opposed to administering several medical/lab tests to all patients who go to the hospital. A battery of tests can be efficient but they can also be expensive and usually ineffective.

Big Data Providers in this industry include: Recombinant Data, Humedica, Explores and Cerner.

- Education- Industry-Specific big data challenges are:

From a technical point of view, a major challenge in the education industry is to incorporate big data from different sources and vendors and to utilize it on platforms that were not designed for the varying data.

On the technical side, there are challenges to integrate data from different sources, on different platforms and from different vendors that were not designed to work with one another.

Politically, issues of privacy and personal data protection associated with big data used for educational purposes are a challenge.

Applications of big data in Education are:
Big data is used quite significantly in higher education. For example, The University of Tasmania. An Australian university with over 26000 students has deployed a Learning and Management System that tracks among other things, when a student logs onto the system, how much time is spent on different pages in the system, as well as the overall progress of a student over time

Big Data Providers in this industry include: Knew ton and Carnegie Learning and MyFit/ Naviance.

- Manufacturing and Natural Resources- Industry-Specific challenges include:

Increasing demand for natural resources including oil, agricultural products, minerals, gas, metals, and so on has led to an increase in the volume, complexity, and velocity of data that is a challenge to handle.

Applications of big data in manufacturing and natural resources

In the natural resources industry, big data allows for predictive modelling to support decision making that has been utilized to ingest and integrate large amounts of data from geospatial data, graphical data, text and temporal data.

Big data has also been used in solving today's manufacturing challenges and to gain competitive advantage among other benefits.

- Government- *Industry-Specific challenges include*

In governments the biggest challenges are the integration and interoperability of big data across different government departments and affiliated organizations.

Applications of big data in Government

In **public services**, big data has a very wide range of applications including: energy exploration, financial market

The Food and Drug analysis, fraud detection, health related research and environmental protection.
Some more specific examples are as follows:

Administration (FDA) is using big data to detect and study patterns of food-related illnesses and diseases. This allows for faster response which has led to faster treatment and less death.

Lack of personalized services, lack of personalized pricing and the lack of targeted services to new segments and to specific market segments are some of the main challenges.

Big Data Providers in this industry include: Sprint, Qualcomm, Octo Telematics, The Climate Corp.

- Retail and Wholesale Trade- *Industry-Specific challenges include:*

From traditional brick and mortar retailers and wholesalers to current day e-commerce traders, the industry has gathered a lot of data over time. This data, derived from customer loyalty cards, POS scanners, RFID etc. is not being used enough to improve customer experiences on the whole.

Applications of big data in the Retail and Wholesale industry

Big data from customer loyalty data, POS, store inventory, local demographics data continues to be gathered by retail and wholesale stores.
In New York's Big Show retail trade conference in 2014, companies like Microsoft, Cisco and IBM pitched the need for the retail industry to utilize big data for analytics and for other uses including:

§ Optimized staffing through data from shopping patterns, local events, and so on
§ Reduced fraud
§ Timely analysis of inventory

Conclusion

Having gone through a vast knowledge about Big Data and industry vertical including how big data plays a role in these industries, here are a few key take-away:

1. There is substantial real spending around big data
2. To capitalize on big data opportunities, you need to:

- Familiarize yourself with and understand industry-specific challenges
- Understand or know the data characteristics of each industry
- Understand where spending is occurring
- Match market needs with your own capabilities and solutions

Vertical industry expertise is key to utilizing big data effectively and efficiently.

References

- www.tutorialspoint.com
- Hadoop for Dummies
  -by Dirk deRoos
  Paul C. Zikopoulous
  Bruce Brown
  Rafael Coss
- Kennedy, M. T. 2008. Getting counted: Markets, media, And reality. American Sociological Koutroumpis, P., & Leiponen

Data Security using RSA Algorithm in Cloud Computing

Santosh Kumar Singh
Assistant Professor, CS & IT Dept., TIPS Dwarka

Abstract:

Cloud computing is an emerging paradigm which has become today's hottest research area due to its ability to reduce the costs associated with computing. In today's era, it is most interesting and enticing technology which is offering the services to its users on demand over the internet. Since Cloud Computing stores the data and disseminated resources in the open environment, security has become the main obstacle which is hampering the deployment of Cloud environments. Even though the Cloud Computing is promising and efficient, there are many challenges for data security as there is no vicinity of the data for the Cloud user. To ensure the security of data, we proposed a method by implementing RSA algorithm. After implementing RSA Algorithm, we have also analyzed the performance of our algorithm based on three parameters namely Time Complexity, Space Complexity and Throughput. In our proposed work, we are using RSA algorithm to encrypt the data to provide security so that only the concerned user can access it. By securing the data, we are not allowing unauthorized access to it. User data is encrypted first and then it is stored in the Cloud. When required user places a request for the data to the Cloud provider, Cloud provider authenticates the user and delivers the data.

Keywords: **Cloud Computing, Data Security, RSA algorithm, Encryption, Decryption, Time complexity, Space complexity, Throughput.**

Introduction

Cloud computing is the key driving force in many small, medium and large sized companies [1-2], and as many cloud users seek the services of cloud computing, the major concern is the security of their data in the cloud. Securing data is always of vital importance and because of the critical nature of cloud computing and the large amounts of complex data it carries, the need is even more important. Hence forth, concerns regarding data privacy and security are proving to be a barrier to the broader uptake of cloud computing services. Every cloud service(s) seeker either an individual or a company should ask the right questions to the cloud provider before hosting their data or applications on the cloud. Prospective cloud providers should let you know; Are they financially sound? Do they have good security policies and procedures in place? Is the infrastructure meant to host your data shared with lots of other users, or will it be segregated by virtualization? As many companies move their data to the cloud the data undergoes many changes and there are many challenges to overcome. To be effective, cloud data security depends on more than simply applying appropriate data security procedures and countermeasures. Computer based security measures mostly capitalizes on user authorization and authentication. Cloud computing has three delivery models named as Saas, Iaas, Paas and four deployment models such as private cloud, public cloud, hybrid cloud and community cloud. As many cloud users seeks the services of cloud computing, the major

concern is the security of their data in the cloud [3]. Data security is always of vital importance and plays an important role in trust worthiness of computing [4]. Due to the critical nature of cloud computing and the large amounts of complex data it carries, the need is even more important [5]. Hence forth, concerns regarding data privacy and security are proving to be a barrier to the broader uptake of cloud computing services [6]. Security and privacy are always a major concern in cloud computing environment [7]. Some of the security issues are Privacy and Confidentiality, Data integrity, Data location and Relocation, Data Availability, Storage, Backup and Recovery [8-9].

The security of data is the prime responsibility of cloud provider. So, for efficient data security we need a mechanism that provides secure data encryption as well as secure shield against data theft. Different researches have focused on the fact that user generally has to access large volumes of data from the cloud in a secured manner. We need some algorithm that will help in efficient and speedy secured data access. In this study we do research on data security issues in cloud and provide a mechanism which ensures data security in cloud in an efficient way decryption. RSA uses two exponents, e and d, where e is public and d is private. Let the plaintext is M and C is cipher text, then at encryption n is a very large number, created during key generation process.

Proposed Work

In our proposed work, we are using RSA algorithm to encrypt the data to provide security so that only the concerned user can access it [16-17]. By securing the data, we are not allowing unauthorized access to it. User data is encrypted first and then it is stored in the Cloud. When required user places a request for the data to the Cloud provider, Cloud provider authenticates the user and delivers the data. In proposed work, we have to implement RSA algorithm and then analyse its performance based on different parameters such as Time complexity, Space complexity and throughput. The proposed work will be carried out using Eclipse IDE with Java to get the results for different evaluation parameters. The implementation of RSA algorithm involves following steps:

- Key Generation
- Encryption
- Decryption

RSA is a block cipher, in which every message is mapped to an integer. RSA consists of Public-Key and Private-Key. In our Cloud environment, Pubic-Key is known to all, whereas Private-Key is known only to the user who originally owns the data. Thus, encryption is done by the Cloud service provider and decryption is done by the Cloud user or consumer. Once the data is encrypted with the Public-Key, it can be decrypted with the corresponding Private-Key only. RSA uses modular exponential for encryption and

Key Generation:

Before the data is encrypted, Key generation should be done. This process is done between the Cloud service provider and the user.

Steps:

1. Choose two distinct prime numbers a and b. For security purposes, the integers a and b should be chosen at random and should be of similar bit length.
2. Compute n = a * b.
3. Compute Euler's totient function, Ø(n) = (a-1) * (b-1).
4. Chose an integer e, such that 1 < e < Ø(n) and greatest common divisor of e , Ø(n) is 1. Now e is released as Public-Key exponent.
5. Now determine d as follows: $d = e^{-1} (\text{mod } Ø(n))$ i.e., d is multiplicate inverse of e mod Ø(n).
6. d is kept as Private-Key component,
So that d * e = 1 mod Ø(n).
7. The Public-Key consists of modulus n and the public exponent e i.e, (e, n).
8. The Private-Key consists of modulus n and the private exponent d, which must be kept secret i.e, (d, n).

Encryption:

Encryption is the process of converting original plain text (data) into cipher text (data).

Steps: 1. Cloud service provider should give or transmit the Public- Key (n, e) to the user who wants to store the data with him or her.
2. User data is now mapped to an integer by using an agreed upon reversible protocol, known as padding scheme.
3. Data is encrypted and the resultant cipher text (data) C is $C = m^e (\text{mod } n)$.
4. This cipher text or encrypted data is now stored with the Cloud service provider.

Decryption:

Decryption is the process of converting the cipher text (data) to the original plain text (data).

Steps:

1. the cloud user requests the Cloud service provider for the data.
2. Cloud service provider verify's the authenticity of the user and gives the encrypted data i.e, C.
3. The Cloud user then decrypts the data by computing, $m = C^d (\text{mod } n)$.
4. Once m is obtained, the user can get back the original data by reversing the padding scheme.

Key Generation:

1. We have chosen two distinct prime numbers a=61 and b=53.
2. Compute n=a*b, thus n=61*53 = 3233.
3. Compute Euler's totient function, Ø(n)=(a-1)*(b-1), Thus Ø(n)=(61-1)*(53-1) = 60*52 = 3120.
4. Chose any integer e, such that 1 < e < 3120 that is coprime to 3120. Here, we chose e=17.
5. Compute d, $d = e^{-1} (\text{mod } Ø(n))$,
Thus $d = 17^{-1} (\text{mod } 3120) = 2753$.
6. Thus the Public-Key is (e, n) = (17, 3233) and the Private- Key is (d, n) = (2753, 3233). This Private-Key is kept secret and it is known only to the user.

Encryption:

1. The Public-Key (17, 3233) is given by the Cloud service provider to the users who wish to store the data.
2. Let us consider that the user mapped the data to an integer m=65.
3. Data is encrypted now by the Cloud service provider by using the corresponding Public-Key which is shared by both the Cloud service provider and the user. $C = 65^{17} (\text{mod } 3233) = 2790$.
4. This encrypted data i.e., cipher text is now stored by the Cloud service provider.

Decryption:

1. When the user requests for the data, Cloud service provider will authenticate the user and delivers the encrypted data (If the user is valid).
2. The cloud user then decrypts the data by computing, $m = C^d (\text{mod } n) = 2790^{2753} (\text{mod } 3233) = 65$.
3. Once the m value is obtained, user will get back the original data.

CONCLUSION

Cloud Computing is still a new and evolving paradigm where computing is regarded as on-demand service. Once the organization takes the decision to move to the cloud, it loses control over the data. Thus, the amount of protection needed to secure data is directly proportional to the value of the data. Security of the Cloud relies on trusted computing and cryptography.

Thus, in our proposed work, only the authorized user can access the data. Even if some intruder (unauthorized user) gets the data accidentally or intentionally if he captures the data also, he can't decrypt it and get back the original data from it.

Refrences

- Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, Bhavani Thuraisingham, "Security Issues for Cloud Computing". The University of Texas at Dallas, USA, International Journal of Information Security and Privacy, 4(2), 39-51, April-June 2010.
- Anup R. Nimje, "Cryptography in Cloud-Security Using DNA (Genetic) Techniques", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue5, pp.1358-1359, Sept- Oct2012.
- Engr: Farhan Bashir Shaikh, Sajjad Haider, "Security Threats in Cloud Computing", 6th International Conference on Internet Technology and Secured Transactions, Abu Dhabi, United Arab Emirates, 11-14 December 2011
- Rachna Arora, Anshu Parashar, "Secure User Data in Cloud Computing Using Encryption Algorithms", International Journal of Engineering Research and Applications (IJERA), ISSN: 2248-9622, www.ijera.com, Vol. 3, Issue 4, pp.1922-1926, Jul-Aug 2013.
- Danish Jamil, Hassan Zaki, "Cloud Computing Security", International Journal of Engineering Science and Technology IJEST, ISSN: 0975-5462, Vol. 3 No. 4, pp. 2672-2676, April2011.
- Dr. P. Dinadayalan, S. Jegadeeswari, Dr. D. Gnanambigai, "Data Security Issues in Cloud Environment and Solutions", World Congress on Computing and Communication Technologies 2014.
- Natan Abolafya, Secure Documents Sharing System for Cloud Environments, Master of Science Thesis Stockholm, Sweden 2012.
- Abdullah Al Hasib, Abul Ahsan Md. Mahmudul Haque, "A Comparative Study of the Performance and Security Issues of AES and RSA Cryptography", Third International Conference on Convergence and Hybrid Information Technology, 2008.
- Cloud Security Alliance, (2009) Security Guidance for Critical Area of Focus in Cloud Computing V2.1. [Online]. Available: https://cloudsecurityalliance.org/csaguide.pdf, accessed on Feb 2012.

Dark Web

Neha Aggarwal

Assistant Professor, CS & IT Dept., TIPS Dwarka

The darknets which constitute the software, configurations, or authorization to access. The dark web forms a small part of the deep web, the part of the Web not indexed by web search engines, although sometimes the term *deep web* is mistakenly used to refer specifically to the dark web.

Dark web include small, friend-to-friend peer-to-peer networks, as well as large, popular networks like Tor, Free net, I2P, and Riffle operated by public organizations and individuals. Users of the dark web refer to the regular web as clear net due to its unencrypted nature. The Tor dark web may be referred to as onionland, a reference to the network's top-level domain suffix .onion and the traffic anonymization technique of onion routing.

Darknet websites are accessible only through networks such as Tor ("The Onion Routing" project) and I2P ("Invisible Internet Project"). Tor browser and Tor-accessible sites are widely used among the darknet users and can be dark web is the World Wide Web content that exists on darknets, overlay networks that use the Internet but require specific identified by the domain ".onion" While Tor focuses on providing anonymous access to the Internet, I2P specializes on allowing anonymous hosting of websites. Identities and locations of darknet users stay anonymous and cannot be tracked due to the layered encryption system.

Botnets

Botnets are often structured with their command and control servers based on a censorship-resistant hidden service, creating a large amount of bot-related traffic.

Bitcoin services

Bitcoin services such as tumblers are often available on Tor, and some – such as Grams – offer darknet market integration.A research study undertaken by Jean-Loup Richet, a research fellow at ESSEC, and carried out with the United Nations Office on Drugs and Crime, highlighted new trends in the use of Bitcoin tumblers for money laundering purposes. A common approach was to use a digital currency exchanger service which converted Bitcoin into an online game currency (such as gold coins

in World of Warcraft) that will later be converted back into money. It has been shown possible that Blockchain and cryptocurrency can be used to regulate the dark web

Darknet markets
Commercial darknet markets, which mediate transactions for illegal drugs and other goods, attracted significant media coverage starting with the popularity of Silk Road and DiabolusMarketand its subsequent seizure by legal authorities. Other markets sell software exploit sand weapons. Examination of price differences in Dark web markets versus prices in real life or over the World Wide Web have been attempted as well as studies in the quality of goods received over the Dark web. One such study was performed on Evolution, one of the most popular crypto-markets active from January 2013 to March 2015. Although it found the digital information, such as concealment methods and shipping country, "seems accurate", the study uncovered issues with the quality of illegal drugs sold in Evolution, stating that, "... the illicit drugs purity is found to be different from the information indicated on their respective listings. Less is known about consumer motivations for accessing these marketplaces and factors associated with their use.

Hacking groups and services
Many hackers sell their services either individually or as a part of groups.Such groups include xDedic, hackforum, Trojanforge, Mazafaka, dark0de and the TheRealDeal darknet market.Some have been known to track and extort apparent pedophiles. Cyber crimes and hacking services for financial institutions and banks have also been offered over the Dark web.Attempts to monitor this activity have been made through various government and private organizations, and an examination of the tools used can be found in the Procedia Computer Science journal.Use of Internet-scale DNS Distributed Reflection Denial of Service (DRDoS) attacks have also been made through leveraging the Dark Web.There are many scam .onion sites also present which end up giving tools for download that are infected with trojan horses or backdoors.

Fraud services
There are numerous carding forums, PayPal and Bitcoin trading websites as well as fraud and counterfeiting services. Many such sites are scams themselves.

Phishing and scams
Phishing via cloned websites and other scam sites are numerous,with darknet markets often advertised with fraudulent URLs.

Puzzles
Puzzles such as Cicada 3301 and successors will sometimes use hidden services in order to more anonymously provide clues, often increasing speculation as to the identity of their creators.

Illegal pornography
There is regular law enforcement action against sites distributing child pornography – often via compromising the site by distributing malware to the users.Sites use complex systems of guides, forums and community regulation. Other content includes sexualised torture and killing of animals and revenge porn.

Terrorism
There are at least some real and fraudulent websites claiming to be used by ISIL (ISIS), including a fake one seized in Operation Onymous. In the wake of the November 2015 Paris attacks an actual such site was hacked by an Anonymous affiliated hacker group GhostSec and replaced with an advert for Prozac. The RawtiShax Islamist group was found to be operating on the dark web at one time.

Social media
Within the dark web, there exist emerging social media platforms similar to those on the World Wide Web. Facebook and other traditional social media platforms have begun to make dark-web versions of their websites to address problems associated with the traditional platforms and to continue their service in all areas of the World Wide Web.

Network Security and Types of Attacks in Network

Shikha Bhalla
Assistant Professor, CS & IT Dept., TIPS Dwarka

Abstract

The computer network technology is developing rapidly, and the development of internet technology is more quickly, people more aware of the importance of the network security. Network security is main issue of computing because many types of attacks are increasing day by day. In mobile ad-hoc network the nodes are independent. Protecting computer and network security are critical issues. The malicious nodes create a problem in the network. This malicious nodes acts as selfishness, It can use the resources of other nodes and preserve the resources of its own. After analyzing and quantifying the network information security elements confidentiality, integrity and availability, this article describes the network security confidentiality vector, network security integrity vector and network security availability vector. This article also covers major type of attacks in MANET.

Introduction

Network security starts with authorization, commonly with a username and a password. Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, modification in system, misuse, or denial of a computer network and network-accessible resources. Basically network security involves the authorization of access to data in a network, which is controlled by the network admin. It has become more important to personal computer users, and organizations. If this authorized, a firewall forces to access policies such as what services are allowed to be accessed for network users. So that to prevent unauthorized access to system, this component may fail to check potentially harmful content such as computer worms or Trojans being transmitted over the network. Anti-virus software or an intrusion detection system (IDS) help detect the malware. Today anomaly may also monitor the network like wire shark traffic and may be logged for audit purposes and for later on high-level analysis in system. Communication between two hosts using a network may be uses encryption to maintain privacy policy. The world is becoming more interconnected of the Internet and new networking technology. There is a so large amount of personal, military, commercial, and government information on networking infrastructures worldwide available. Network security is becoming of great importance because of intellectual property that can be easily acquired through the internet. The network security is analyzed by researching the following:

- History of network security
- Internet architecture and security aspects of the Internet
- Types of network attacks and security methods
- Security for internet access in networks
- Current development in the network security hardware and software

Network Security System and Network Technology is a key technology for a wide variety of applications. It is a critical requirement in current situation networks, there is a significant lack of security methods that can be easily implemented. There exists a "communication gap" between the developers of security technology and developers of networks. Network design is a developed process that is depends on the Open Systems Interface (OSI) model. The OSI model has several advantages when designing network security. It offers modularity, ease of use, flexibility, and standardization of protocols. The protocols of different layers can be easily combined to create stacks which allow modular development. In contrast to secure network design is not a well developed process. There isn't a methodology to manage the complexity of security requirements. When considering about network security, it should be emphasized that the complete network is secure. It does not only concern with the security in the computers at each end of the communication chain. When transferring from one node to another node data the communication channel should not be vulnerable to attack. A hacker will target the communication channel, get the data, and decrypt it and reinsert a duplicate message. Though securing the network is just as important as securing the computers and encrypting the message. While developing a secure network, the following needs to be considered.

2.1 Confidentiality It means that the non-authenticated party does not examine the data.

2.2 Integrity It is an guarantee that the data which is received by the receiver has not been change or Modified

after the send by the sender.

3. Types of Attacks Here we are presenting some basic class of attacks which can be a cause for slow network performance, uncontrolled traffic, viruses etc. Attacks to network from malicious nodes. Attacks can be categories in two"Passive" when a network intruder intercepts data traveling through the network, and "Active" in which an intruder initiates commands to disrupt the network's normal operation.

3.1. Active attack Some active attacks are spoofing attack, Wormhole attack, Modification, Denial of services, Sinkhole, and Sybil attack.

a. Spoofing: When a malicious node miss-present his identity, so that the sender change the topology

b. Modification: When malicious node performs some modification in the routing route, so that sender sends the message through the long route. This attack cause communication delay occurred between sender and receiver.

c. Wormhole: This attack is also called the tunnelling attack. In this attack an attacker receives a packet at one point and tunnels it to another malicious node in the network. So that a beginner assumes that he found the shortest path in the network.

d. Fabrication: A malicious node generates the false routing message. This means it generate the incorrect information about the route between devices.

e. Denial of services: In denial of services attack, malicious node sending the message to the node and consume the bandwidth of the network. The main aim of the malicious node is to be busy the network node.
If a message from unauthenticated node will come, then receiver will not receive that message because he is busy and beginner has to wait for the receiver response.

f. Sinkhole: Sinkhole is a service attack that prevents the base station from obtaining complete and correct information. In this attack, a node tries to attract the data to it from his all neighbouring node. Selective modification, forwarding or dropping of data can be done by using this attack .

g. Sybil: This attack related to the multiple copies of malicious nodes. The Sybil attack can be happen due to malicious node shares its secret key with other malicious nodes. In this way the number of malicious node is increased in the network and the probability of the attack is also increases. If we used the multipath routing, then the possibility of selecting a path malicious node will be increased in the network.

3.2. Passive attack: The names of some passive attacks are traffic analysis, Eavesdropping, and Monitoring.

a. Traffic analysis In the traffic analysis attack, an attacker tries to sense the communication path between the sender and receiver. An attacker can found the amount of data which is travel from the route of sender and receiver. There is no modification in data by the traffic analysis.

b. Eavesdropping This is a passive attack, which occurred in the mobile ad-hoc network. The main aim of this attack is to find out some secret or confidential information from communication. This secrete information may be privet or public key of sender or receiver or any secrete data.

c. Monitoring In this attack in which attacker can read the confidential data, but he cannot edit the data or cannot modify the data.

3.3Advance attacks

a. Black hole attack Black hole attack is one of the advance attacking which attacker uses the routing protocol to advertise itself as having the best path to the node whose packets it want to intercept. An hacker use the flooding based protocol for listing the request for a route from the initiator, then hacker create a reply message he has the shortest path to the receiver . As this message from the hacker reached to the initiator before the reply from the actual node, then initiator wills consider that, it is the shortest path to the receiver. So that a malicious fake route is create.

b. Rushing attack In rushing attack, when sender send packet to the receiver, then attacker alter the packet and forward to receiver. Attacker performs duplicate sends the duplicate to the receiver again and again. Receiver assumes that packets come from sender so the receiver becomes busy continuously.

c. Replay attack It this attack a malicious node may repeat the data or delayed the data. This can be done by originator who intercept the data and retransmit it. At that time, an attacker an intercept the password.

d. Byzantine attack A set of intermediate node works between the sender and receiver and perform some changes such as creating routing loops, sending packet through non optimal path or selectively dropping packet, which result in disruption or degradation of routing services.

e. Location disclosure attack Malicious node collects the information about the node and about the route by computing and monitoring the traffic. So malicious node may perform more attack on the network.

Conclusion

The security is the main problem in the mobile ad-hoc network. In MANNET node looks like selfishness. A node can use the resources of other node and preserve the resources of own. This type of node creates the problem in MANET there are a number of ways, which guarantee for the safety and security of your network. Perform the following to avoid security loopholes. Must have an updated antivirus program. Don't provide more or unwanted access to any network user. Operating system should be regularly updated.

Cyber Crime

Shruti Bajaj

Assistant Professor, CS & IT Dept., TIPS Dwarka

Cybercrime, or **computer-oriented crime**, is the crime that involves a computer and a network.The computer may have been used in the commission of a crime, or it may be the target.Cybercrimes can be defined as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS). Cybercrime may threaten a person or a nation's security and financial health.

Issues surrounding these types of crimes have become high-profile, particularly those surrounding hacking, copyright infringement, unwarranted mass-surveillance, child pornography, and child grooming.There are also problems of privacy when confidential information is intercepted or disclosed, lawfully or otherwise.

Classifications:-

Financial fraud crimes

Computer fraud is any dishonest misrepresentation of fact intended to let another to do or refrain from doing something which causes loss. Altering in an unauthorized way. This requires little technical expertise and is common form of theft by employees altering the data before entry or entering false data, or by entering unauthorized instructions or using unauthorized processes;

- Altering, destroying, suppressing, or stealing output, usually to conceal unauthorized transactions. This is difficult to detect;
- Altering or deleting stored data.

Cyber terrorism

Cyber terrorism in general can be defined as an act of terrorism committed through the use of cyberspace or computer resources (Parker 1983). As such, a simple propaganda piece in the Internet that there will be bomb attacks during the holidays can be considered cyber terrorism. There are also hacking activities directed towards individuals, families, organized by groups within networks, tending to cause fear among people, demonstrate power, collecting information relevant for ruining peoples' lives, robberies, blackmailing etc.

Cyberextortion:

Cyber-extortion occurs when a website, e-mail server, or computer system is subjected to or threatened with repeated denial of service or other attacks by malicious hackers. These hackers demand money in return for promising to stop the attacks and to offer "protection". According to the Federal Bureau of Investigation, cyber crime extortionists are increasingly attacking corporate website and networks, crippling their ability to operate and demanding payments to restore their service. More than 20 cases are reported each month to the FBI and many go unreported in order to keep the victim's name out of the public domain. An example of cyber-extortion was the attack on Sony Pictures of 2014.

Cyber Warfare:

The U.S. Department of Defense (DoD) notes that the cyberspace has emerged as a national-level concern

through several recent events of geostrategic significance. Among those are included, the attack on Estonia's infrastructure in 2007, allegedly by Russian hackers. "In August 2008, Russia again allegedly conducted cyber-attacks, this time in a coordinated and synchronized kinetic and non-kinetic campaign against the country of Georgia.

Computer as a target:

These crimes are committed by a selected group of criminals. Unlike crimes using the computer as a tool, these crimes require the technical knowledge of the perpetrators. As such, as technology evolves, so too does the nature of the crime. These crimes are relatively new, having been in existence for only as long as computers have—which explains how unprepared society and the world in general is towards combating these crimes. There are numerous crimes of this nature committed daily on the internet.

Crimes that primarily target computer networks or devices include:

- Computer viruses
- Denial-of-service attacks
- Malware (malicious code)

Combating Computer Crime

Diffusion of cybercrime

The broad diffusion of cybercriminal activities is an issue in computer crimes detection and prosecution. According to Jean-Loup Richet (Research Fellow at ESSEC ISIS), technical expertise and accessibility no longer act as barriers to entry into cybercrime.Indeed, hacking is much less complex than it was a few years ago, as hacking communities have greatly diffused their knowledge through the Internet. Blogs and communities have hugely contributed to information sharing: beginners could benefit from older hackers' knowledge and advice. Furthermore, hacking is cheaper than ever: before the cloud computing era, in order to spam or scam one needed a dedicated server, skills in server management, network configuration, and maintenance, knowledge of Internet service provider standards, etc.

Investigation

A computer can be a source of evidence (see digital forensics). Even where a computer is not directly used for criminal purposes, it may contain records of value to criminal investigators in the form of a logfile. In most countriesInternet Service Providers are required, by law, to keep their logfiles for a predetermined amount of time. For example; a European wide Data Retention Directive (applicable to all EU member states) states that all e-mail traffic should be retained for a minimum of 12 months.

Legislation

Due to easily exploitable laws, cybercriminals use developing countries in order to evade detection and prosecution from law enforcement. In developing countries, such as the Philippines, laws against cybercrime are weak or sometimes nonexistent. These weak laws allow cybercriminals to strike from international borders and remain undetected. Even when identified, these criminals avoid being punished or extradited to a country, such as the United States, that has developed laws that allow for prosecution. While this proves difficult in some cases, agencies, such as the FBI, have used deception and subterfuge to catch criminals. For example, two Russian hackers had been evading the FBI for some time.

Penalties

Penalties for computer-related crimes in New York State can range from a fine and a short period of jail time for a Class A misdemeanor such as unauthorized use of a computer up to computer tampering in the first degree which is a Class C felony and can carry 3 to 15 years in prison.

However, some hackers have been hired as information security experts by private companies due to their inside knowledge of computer crime, a phenomenon which theoretically could create perverse incentives. A possible counter to this is for courts to ban convicted hackers from using the Internet or computers, even after they have been released from prison – though as computers and the Internet become more and more central to everyday life, this type of punishment may be viewed as more and more harsh and draconian.

Awareness

As technology advances and more people rely on the internet to store sensitive information such as banking or credit card information, criminals increasingly attempt to steal that information. Cybercrime is becoming more of a threat to people across the world. Raising awareness about how information is being protected and the tactics

criminals use to steal that information continues to grow in importance. According to the FBI's Internet Crime Complaint Center in 2014, there were 269,422 complaints filed. There are 1.5 million cyber-attacks annually that means that there are over 4,000 attacks a day, 170 attacks every hour, or nearly three attacks every minute, with studies showing only 16% of victims had asked the people who were carrying out the attacks to stop.