Jan - Jul 2020

TRINITY INSTITUTE OF PROFESSIONAL STUDIES

Dwarka, Sector-9, New Delhi

Trinity Tech Review

Vol 6, Issue 1

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, the 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
ISO 9001:2008 Certified
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	:	Bi - Annually
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. Barkha Bahl
	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

Cloud Computing Security Using Steganography

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

lintroduction

Cloud computing provides the ability to use computing and storage resources on a rented basis and reduces investments in an organization's computing infrastructure. With huge benefits cloud computing also brings with it concerns about the security and privacy of information. Nowadays cloud computing is used by smart mobile applications so there are some security and privacy concerns on data provided by cloud providers. In this paper, we demonstrate how Steganography, which is a secrecy method to conceal information, can be used to enhance the security and privacy of data maintained on the cloud by mobile applications. Our proposed design works with a key, which is securely surrounded in the image along with the data, to provide an additional layer of security.
Cloud computing is a recent development in information technology that moves computing and data away from desktop and portable PCs into a large data centre. Cloud refers to applications delivered as services over the internet as well as to the actual cloud infrastructure namely, the hardware and systems software in data centers that provide these services [1].

In [2], a combined approach of steganography with LSB encoding technique and Data Encryption Standard algorithm (DES). In which they encrypted data by DES encryption algorithm and then embedded the decrypted data by the LSB method. As LSB is not much secure enough, we can say that this system doesn't provide better security. An advanced technique to share and protect cloud data using multilayer steganography and cryptography is used in [3]. Where data is encrypted by the AES (Advanced Encryption Standard) algorithm, and then encrypted data embedded in a cover image by using the Hash-LSB algorithm.

Steganography

Steganography implies concealing data or information, it allowing data/information to be transferred to the receiver end without knowing that the original message still existed. The processes generally imply placing a hidden message within some transport medium. Steganography is fully different from cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages which transforms a message into a non-understandable string that can only be deciphered by the recipient end. As in cryptography, it is normal that a data/information in the form of a message has been sent, but the data/information of the message is interchanged. As in steganography, the casual observer has no idea that a data/information in the form of a message had been sent.

Figure 1 showing the architecture of Mobile Cloud Computing. In Figure 1, the main parts or components of the Mobile Cloud Computing architecture are mobile users with an internet connection, smart mobile device, and cloud service provider which is the essential part of architecture [5]. Figure 2 represents the steganography architecture.

Stego Application will take as an input of Cover file and Data to hide and produce after the process as a stego file. The First input is a cover file which may be in the form of image, video, or audio and the second input is data to hide which may include in the form of text, image, video, audio, etc, after inputting the inputs into stego application it will process the data and produce stego file which will be secure and safe.

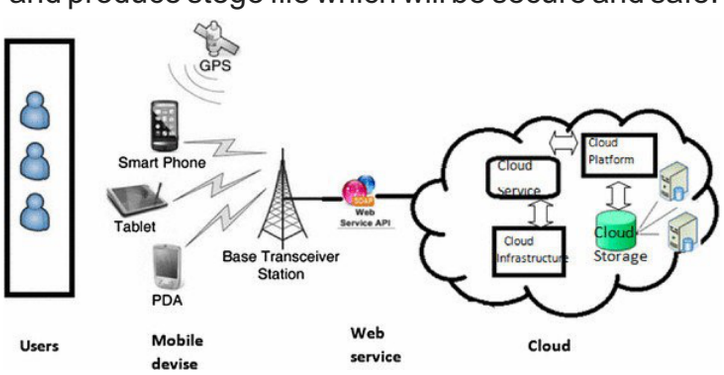


Figure1. Mobile cloud computing

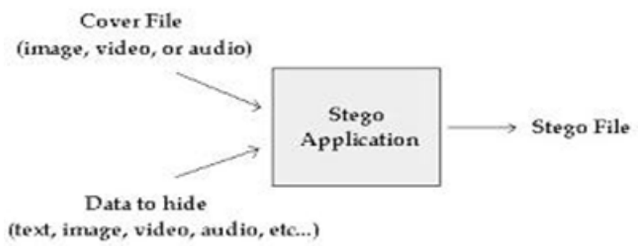


Figure2. The architecture of Steganography

Methods of Steganography

Generally, the most common approaches for information hiding are: (1) Least Significant Bit (LSB) insertion, (2) Masking and filtering techniques, (3) Algorithms and Transformation [4].

Basically steganography applications with the LSB method of substitution randomly take which bits will be used for the process in steganography. More developed applications first evaluate the carrier image and set the boundaries which bits should be altered to minimize detection and maintain the original aspect of the image [7].

Proposed Approach to Secure Data from Cloud Provider

Software working model of the proposed system with the steganography application (SA) shown in Figure 3. The main component of our model includes the following components -

- User- the role of the user is to select an image and combination of key and data. Smart Mobile device- able to run steganography application
- Steganography application – used to encapsulate data and the key in the image provided by the user.
- Stego image- Steganography application produces a stego image which we send to the cloud. After that software retrieves data from the image if a user's entered key matched.

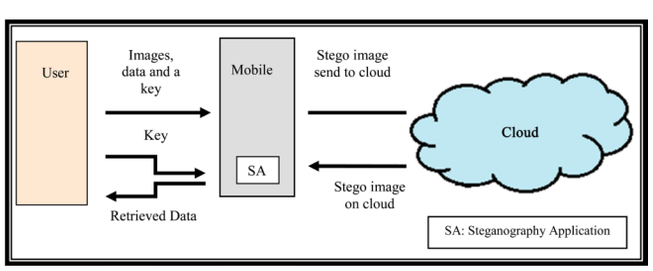


Figure3. Proposed system

The proposed system is a combination of cloud computing and steganography. In this model, the user will select an image, after that enter the data and the keys as the input now this input will be used by the steganography application, which is installed on the user's mobile device. The steganography application converts the inputs and produces a stego image to be accumulated on the cloud. As we know, an internet connection is a must for cloud access. When users want to access the data which is on the cloud he has to use a steganography application and he has to input the key, if the key matched then the user easily and safely access the data.

In this paper, we have used the least significant bit technique to hide information, which makes the mobile cloud computing application robust, dynamic, and least concerned for image misrepresentation. Further, we will use 24-bit images which makes possible of 16,000k different combinations that can easily conceal data in a way that it will be quite tough to detect any difference between the modified image and the original image or actual image.

Implementation

Basically, mobile phones are much easier to access our online accounts and users prefer mobile applications for their work. So he has a number of accounts, their login id and passwords and there is a chance to forget these login id and passwords. In such situations users can store a limited amount of information or data on the cloud, by mobile using steganography, which will secure user data from cloud administrators. If a user or customer is storing their information on the cloud then they can easily access data from any location without any tension of losing important data.

This application is suitable for low amounts of data with less processing power and low battery usage. Therefore it increases the performance of the overall application and the mobile device. This approach combines and improves the trust in mobile computing as well as improves the efficiency of cloud computing, so that users can use mobile applications in a more secure way without any tension of data damage.

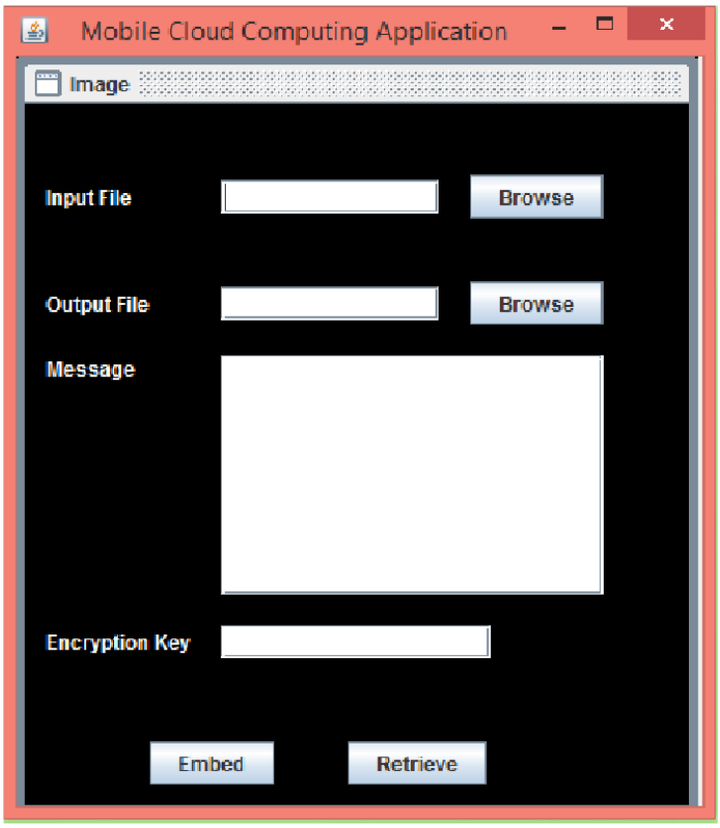


Figure4. Home page

The Above Figure4 shows the Mobile Cloud Computing Applications home page, there is a facility to choose input and output image path and it depends upon the user where the user can select an input and output image path, and enter data and a key encapsulated into an image.

Below Figure 5 is the original image as an input on which software works and converts it into stego image and Figure 6 is the stego image which is the converted form of original image created after encapsulated secret message and the key. Image is little changed but it cannot be identified by normal human eyes.

Conclusion and Future Work

In this paper, a proposed steganography application can be used for data security without others' involvement. The proposed system will work efficiently with the key. But if he/she loses the key, then the system does not have any provision to recover the key, so in this case a user might lose the data. This is the serious drawback on which we will work in future. The Proposed system is only applicable for limited data so in future we will try large data processing. In the future we can say, cloud and proposed models will work together in an efficient manner.

References

1. Singh, S. K., Manjhi, P.K., Tiwari, R.K., and Vadi, V. 2018, A Secure Communication Scheme for Cloud Environment. International Journal of Computer Engineering and Applications, vol. 12, issue 4, pp. 97-106.

2. Karthikeyan, B., Deepak, A. K., S., Subalakshmi, A., and Vaithiyanathan, V. 2017, A combined approach of steganography with LSB encoding technique and DES algorithm", Proc. of 3rd International Conference on
Advances in Electrical, Electronics, Information, Communication and BioInformatics.

3. Ranjan, A. and Bhonsle, M. 2016, Advanced technics to shared & protect cloud data using multilayer steganography and cryptography", Proc. of IEEE International Conference on Automatic Control and Dynamic Optimization Techniques.

4. Kumar, A. and Pooja, K. 2010, Steganography: A Data Hiding Technique. International Journal of Computer Applications, 975-8887. http://dx.doi.org/10.5120/1398-1887

5. Shamim, S., Sarker, A. and Bahar, A. 2015, A Review on Mobile Cloud Computing. International Journal of Computer Applications, 113, 4-9. http://dx.doi.org/10.5120/19908-1883

6. Mahajan, S. and Singh, A. 2012, A Review of Methods and Approach for Secure Steganography. International Journal of Advanced Research in Computer Science and Software Engineering, 2, 484-488.

https://cyber-defense.sans.org/resources/papers/gsec/steganography-corporate-environment-106511 7.

8. Hanen Jemal, Kechaou Zied and A. B. Mounir. 19th july 2016, An enhanced healthcare in mobile cloud computing environment, Springerlink.com, DOI 10.1007/s40595-016-0076-y.

Smart Computing based Solutions

Ms. Ritika Kapoor
Assistant Professor, CS&IT Department, TIPS Dwarka

Introduction to Smart Computing

The technology industry has entered a new phase of tech innovation and growth, which is known as "Smart Computing." We evolved on computing over a period of time i.e. started with giant mainframe computers where the processing was centralized and computing was more restricted to some government and mission-critical research applications. As part of the evolution, personal computing slowly started penetrating into all walks of our lives starting from healthcare, education, finance, transportation, etc. This all made life simple and easy, and at the same time there are some inherent challenges too with respect to security, and maintainability as we started embracing technology more. The Internet of Things revolves around increased machine-to-machine communication, and it's said that this technology will make everything from streetlights to seaports “smart.” Its true value lies in the intersection of gathering data and analyzing it. Today, there's a huge network of physical objects that are embedded with electronics, software, sensors and connectivity. These objects, or “things”, are able to both collect and exchange data, and the network will only continue to grow in coming years. In really simple terms, the Internet of Things is all about connecting devices and objects over the Internet. They are able to talk to each other and us. There are plenty of examples already: smart technology in automobiles, the smart fridge, mobile devices, wearable technology, and so much more. And IoT isn't even limited to singular devices. Imagine a truly smart home, or an entire smart city.

The Challenges

Security is always a top concern when new technology is introduced. It's extremely valid, as devices within the IoT will certainly be gathering a lot of data about people. This is a challenge that experts in the Internet of Things are already working to overcome, and it's still in the early stages. There have not yet been excessive hackings, but as IoT develops, it will be more attractive to hackers – this means more emphasis should be put on security in these early stages to avoid problems later. However, it's important to keep in mind that these devices are just as susceptible as a home PC or smartphone – it's all on an even playing field. And as the Internet of Things grows, so will security technology.

Another concern is how the Internet of Things will affect business. Some think it will affect productivity levels or lead to an invasion of worker privacy. IoT will almost definitely impact how business is done today, but it can have a positive impact. Manufacturing already uses the Internet of Things to organize and track machines, while farmers are able to monitor their crops and cattle. As more and more businesses adopt this technology, it can have a significant impact on production and efficiency. And while employees may not like the idea of being tracked throughout the workday, this concern may lead to the implementation of IoT policies to both protect workers and take advantage of the latest technology.

Application Domains of IOT

IoT applications promise to bring immense value into our lives. With newer wireless networks, superior sensors and revolutionary computing capabilities, the Internet of Things could be the next frontier in the race for its share of the wallet.

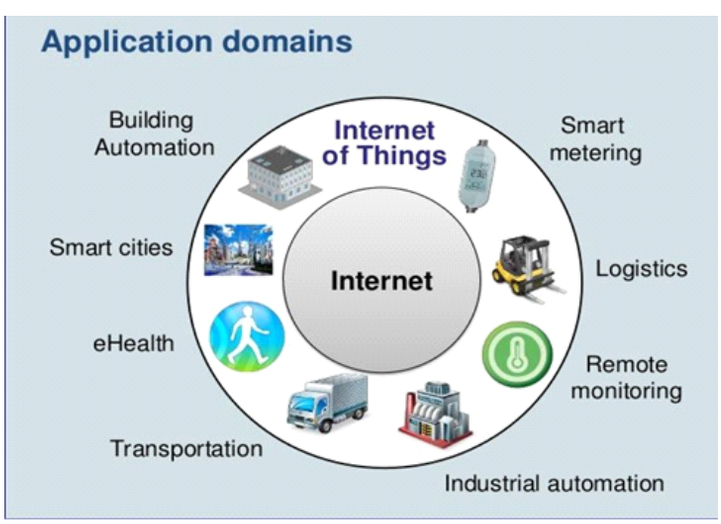


Fig 1: Internet of Things in various Domains

- Building Automation: - The IoT is now starting to have a transformative effect on smart building automation and control. By disrupting long-established business models and offering significant new opportunities to improve the efficiency of buildings, the IoT can raise employee productivity as well as stimulating the development of innovative services.
- Smart Cities: - A smart city is an urban area that uses different types of electronic Internet of things (IoT) sensors to collect data. Insights gained from that data are used to manage assets, resources, and services efficiently. Smart city includes traffic management to water distribution, to waste management, urban security, and environmental monitoring.
- eHealth: - IoT in Healthcare is a heterogeneous computing, wirelessly communicating system of apps and devices that connects patients and health providers to diagnose, monitor, track and store vital statistics and medical information.
- Transportation:-IoT devices are deployed in traffic congestion control systems, telematics systems within motor vehicles, in reservation and booking systems used by transport operators, in security and surveillance systems, and in remote vehicle monitoring systems.
- Industrial automation: - Industrial automation companies that utilize IoT solutions can realize new advantages. The Internet of Things (IoT) assists to generate new technologies to resolve problems, improve operations and enhance productivity. The IoT can be described as the connection of only known electronic devices using Internet 'data plumbing' involving Internet Protocol (IP), web services, and cloud computing.
- Remote monitoring: - Remote monitoring using IoT uses a web-based technology like a Global Positioning System (GPS) receiver and an onboard communication device on each machine. The GPS receiver identifies the machine location, while the communication device collects the information sent to it by sensors on the machine.
- Logistics: - IoT plays an integral part in the growth of the logistics industry. It provides for smarter warehouse management by tightening supply processes using sensors and intelligence devices.
- Smart Metering: - A smart meter is an electronic device that allows for remote monitoring and recording of energy consumption. However, in the age of IoT and IoT platforms, standalone smart meters give way to more advanced and multi-purpose smart metering solutions. These solutions offer a broader range of remote monitoring and alerting capabilities as well as provide powerful data analytics tools to help companies and individual users optimize their energy, water, gas, or fuel consumption.

References:

- https://medium.com/datadriveninvestor/what-is-smart-in-smart-computing-6a5de3f5ebe0
- https://www.forrester.com/report/Smart+Computing+Drives+The+New+Era+Of+IT+Growth/-/E-RES55157
- https://mobility.here.com/learn/smart-transportation/iot-transportation-benefits-challenges-and-uses
- https://thingsboard.io/smart-metering/
- https://smartbuildingsmagazine.com/features/iot-and-its-uses-in-buildings
- https://link.springer.com/article/10.1007/s11280-019-00773-y

Natural Language Processing

Ms. Saba Hussain
Assistant Professor, CS&IT Department, TIPS Dwarka

Natural Language Processing or NLP is a field of Artificial Intelligence that gives the machines the ability to read, understand and derive meaning from human languages. It is a discipline that focuses on the interaction between data science and human language and is scaling to lots of industries. Today NLP is booming due to huge improvements in the access to data and the increase in computational power, which are allowing practitioners to achieve meaningful results in areas like healthcare, media, finance, and human resources, among others.

Data generated from conversations, declarations, or even tweets are examples of unstructured data. Unstructured data doesn't fit neatly into the traditional row and column structure of relational databases, and represent the vast majority of data available in the actual world. It is messy and hard to manipulate. Nevertheless, thanks to the advances in disciplines like machine learning a big revolution is going on regarding this topic. Nowadays it is no longer about trying to interpret a text or speech based on its keywords (the old-fashioned mechanical way), but about understanding the meaning behind those words (the cognitive way). This way it is possible to detect figures of speech like irony or even perform sentiment analysis.

NLP can help us with lots of tasks and the fields of application just seem to increase on a daily basis. Here are few examples:

1. Handling large volumes of text data

With the help of NLP, users can analyse more data than ever, including for critical processes like medical research. This technology is especially important now, as researchers attempt to find a vaccine for COVID-19. In a recent article, the World Economic Forum (WEF) points out that NLP can help researchers tackle COVID-19 by going through vast amounts of data that would be impossible for humans to analyse. Machines can find, evaluate, and summarise the tens of thousands of research papers on coronavirus, to which thousands are added every week. In addition, this technology can help track the spread of the virus by detecting new outbreaks.

1. Prediction of Diseases

NLP enables the recognition and prediction of diseases based on electronic health records and patient's own speech. This capability is being explored in health conditions that go from cardiovascular diseases to depression and even schizophrenia. For example, Amazon Comprehend Medical is a service that uses NLP to extract disease conditions, medications, and treatment outcomes from patient notes, clinical trial reports, and other electronic health records.

2. Chatbots

A lot of Industry analysts predict that Chatbots are an emergent trend that will offer real-time solutions for simple customer service problems. They are unquestionably gaining a lot of trust and popularity from the consumer as well as engineers. They are useful in providing standard solutions to common problems. Chatbots help save time, human efforts, cost and provide efficient solutions and keep improving from learning from time to time.

3. Managing the Advertisement Funnel

What does the consumer need? Where is the consumer looking for his or her needs? Natural Language Processing is a great source for intelligent targeting and placement of advertisements in the right place at the right time and for the right audience. Reaching out to the right patron of your product is the ultimate goal for any business. NLP matches the right keywords in the text and helps to hit the right customers.

4. Voice Driven Interfaces

Amazon's Alexa and Apple's Siri are examples of intelligent voice-driven interfaces that use NLP to respond to vocal prompts and do everything like find a particular shop, tell us the weather forecast, suggest the best route to the office or turn on the lights at home.

Improvement Area of NLP

The main drawbacks we face these days with NLP relate to the fact that language is very tricky. The process of understanding and manipulating language is extremely complex, and for this reason, it is common to use different techniques to handle different challenges before binding everything together. It is a known issue that while there is tons of data for popular languages, such as English or Chinese but there are thousands of languages that are spoken around the world but receive far less attention. The data for these languages are scarce. So, maintaining and processing vocabularies, dialects of such languages is a research area.
Also, one of the major challenges of NLP is the understanding and modelling of elements within a variable context. In a natural language, words are unique but can have different meanings depending on the context resulting in ambiguity on the lexical, syntactic, and semantic levels. To solve this problem, NLP offers several methods, such as evaluating the context or introducing Part of Speech (POS) tagging, however, understanding the semantic meaning of the words in a phrase remains an open task.

Why NLP will be the future?

A significant reward of NLP to businesses is the concept of a smart assistant, which has the potential to transform the customer experience, leading to customer loyalty. Smart assistants have already proved their usefulness in customer service.

NLP is paving the way to a brighter future for healthcare delivery and patient experience. It will not be long before it enables physicians to invest their maximum time in patient care while helping them make informed decisions based on real-time, accurate data. NLP is also reducing the time spent in administrative activities by automating workflows.

In addition to addressing health problems, NLP used in conjunction with other artificial intelligence areas can help professionals solve other global challenges, such as clean energy, global hunger, improving education, and natural disasters. For example, according to a Council Post appearing on Forbes, Huge companies like Google are setting their sights on flood prevention, utilizing AI to predetermine areas of risk and notify people in impacted areas.

As regards natural language processing, the sky's the limit. The future is going to see some massive changes as the technology becomes more mainstream and more advancements in the ability are explored. .

REFERENCES:

1 . https://www.kdnuggets.com/2020/08/natural-language-processing-changing-data-analytics.html

2 . https://www.datasciencecentral.com/profiles/blogs/your-guide-to-natural-language-processing-nlp

3. https://www.upgrad.com/blog/5-applications-of-natural-language-processing-for-businesses/

4. https://towardsdatascience.com/why-nlp-is-important-and-itll-be-the-future-our-future-59d7b1600dda

5. https://medium.com/sciforce/biggest-open-problems-in-natural-language-processing-7eb101ccfc9

Analysis of Cryptography Encryption for Network Security

Ms. Upasana Singh
Assistant Professor, CS & IT Dept., TIPS Dwarka

Abstract:
In order to secure network and data transmission via a wireless network, cryptography and network encryption is being used. Providing data protection is one of the key aspects of wireless network data transmission. There are sensors in the wireless networks; they are linked to the base station. The need for protection of the wireless network sensor is very critical, and encryption and network security are necessary. Network security includes security for the terminal system as well as for the whole network system. Network security is one of the main concerns as the world transitions into the digital world. Security of the network provides security for administrator-managed data. Increasing communication technology also requires safe communication which is met through various encryption techniques such as cryptography, digital signatures, watermarking, steganography, and other applications. The cryptography applications range has expanded a lot in the modern area after the development of communication means; cryptography is essentially required to ensure that data are protected against penetrations and to prevent espionage.

Key Terms: Cryptography, Security Services, Security Attacks, Symmetric cipher, Asymmetric Cipher, RSA

INTRODUCTION

Computer data also moves from computer to device, leaving their physical environment safe. When the data is out of control, it is for the fun or benefit of people with poor intentions that the data can be altered or forged. Cryptography can turn and reformat our data to make its journey between computers more secure. The technology is built on secret codes, which are enhanced by modern mathematics that powerfully protect our data. Cryptography means “secret writing” which is the science and art of transforming messages to make them secure and immune to attacks by an unauthorized user. The original data/message, before being transformed is called ciphertext. An encryption is a process to transform the plain text into ciphertext and decryption transforms the ciphertext back into plaintext. The sender uses an encryption algorithm and the receiver uses a decryption algorithm. Thus, encryption and decryption help to secure the transmission of the message and protect the message from unauthorized users.

Cryptography security goals

a. Confidentiality: Confidentiality is probably the most common aspect of information security. We need to protect our confidential information. An organization needs to guard against those malicious actions that endanger the confidentiality of its information.

b. Integrity: Information needs to be changed constantly. Integrity means that changes need to be done only by authorized entities and through authorized mechanisms.

c. Availability: The information created and stored by an organization needs to be available to authorized entities. Information needs to be constantly changed, which means it must be accessible to authorized entities.

NETWORK SECURITY

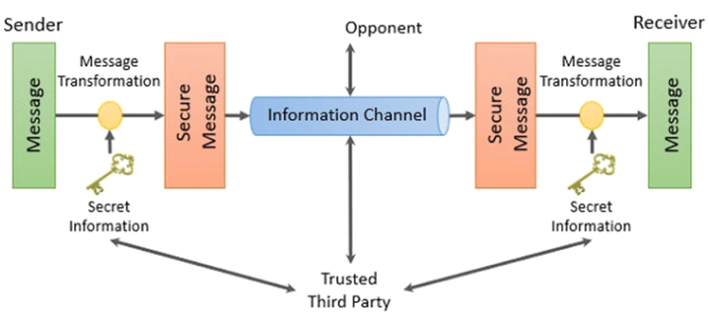
Literature Review

Defense is a wide variety of subjects and encompasses several sins. The goal is to ensure that nobody can read or, worse, alter messages secretly for others. In its simplest shape. It's a matter of people wanting to use remote resources that they can't use. The majority of threats to security are intentionally created by malicious people who try to gain some benefit, care, or damage others. However, the ability of network overall defense at the national level to attack risk is still relatively weak. How to prevent organized malicious network attacks has become a hot topic in the field of security. Studies on network security have started since the birth of information networks. The exponential growth of network size and application, especially the random dynamic access relationship built on the static Internet physical connection network based on the OSI model, makes the study of network more

security more complicated. Before the 1960s, the focus on network security research was how to build an absolute security system and reduce design vulnerabilities to ensure the confidentiality, integrity, and availability of the system, which can be regarded as the first stage of network security research. However, people soon realized the impossibility of practical operation.

Network Security

Model Figure demonstrates the model of system security. A message is to be exchanged starting with one gathering then onto the next over some kind of Internet administration. An outsider might be in charge of appropriating the mystery data to the sender and beneficiary while keeping it from any rival. While building up a safe system, the accompanying should be considered.



Network Security Model

Network security Types

Network security typically consists of three different controls: physical, technical and administrative. Here is a brief description of the different types of network security and how each control works.

Physical Network Security

Physical security controls are designed to prevent unauthorized personnel from gaining physical access to network components such as routers, cabling cupboards and so on. Controlled access, such as locks, biometric authentication and other devices, is essential in any organization.

Technical Network Security

Technical security controls protect data that is stored on the network or which is in transit across, into or out of the network. Protection is twofold; it needs to protect data and systems from unauthorized personnel, and it also needs to protect against malicious activities from employees.

Administrative Network Security

Administrative security controls consist of security policies and processes that control user behavior, including how users are authenticated, their level of access and also how IT staff members implement changes to the infrastructure.

Confidentiality

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

Integrity

- It is a certification that the information which is gotten by the collector has not been a change or Modified after the send by the sender. All the techniques for providing security have two components
- A security-related change on the data to be sent. The Message ought to be scrambled by key with the goal that it is confused by the adversary.
- An encryption enter utilized as a part of conjunction with the change to scramble the message before transmission and unscramble it on gathering Security perspectives become an integral factor when it is fundamental or alluring to shield the data transmission from a rival who may display a danger to classification, realness, etc.

CONCLUSION

Cryptography is a key component for providing protection for network-to-network data communication. It used data against unauthorized users to protect them. The key can be shared more securely between sender and recipient. Security data can be preserved by using techniques like cryptography, watermarking, digital signatures, firewalls, etc. The importance of secure communication has led to cryptographic systems becoming popular so that we can assume that cryptography has proven to be a key to safeguarding our confidential information. The key to building a secure network is to define what security means to your need for the time and use. Once that has been defined, everything that goes on with the network can be evaluated with respect to that policy.

REFERENCES

[1] Zhijie Liu Xiaoyao Xie, Member , IEEE ,School of Mathematics and Computer Science and Zhen Wang, Key Laboratory of Information Computing Science of Guizhou Province , Guizhou Normal University Guiyang , China, The Research of Network Security Technologies.

[2] S.E. Smaha, Haystack: an intrusion detection system[A]. Aerospace Computer Security Applications Conference[C] (IEEE, 2002), pp. 37–44

[3] https://jwcn-eurasipjournals.springeropen.com/articles/10.1186/s13638-019-1506-1

[4] J.P. Anderson, Computer security threat monitoring and surveillance[A] (James P Anderson Co Fort [C], Washington, 1980), pp. 26–32

[5] The Research of Firewall Technology in Computer Network Security, 2009 Second Asia-Pacific Conference on Computational Intelligence and Industrial Applications by Xin Vue, Wei Chen, Yantao Wang, College of Computer and Information Engineering Heilongjiang Institute of Science and Technology Harbin, China.

[6] Shyam Nandan Kumar, “Technique for Security of Multimedia using Neural Network,” Paper id-IJRETM-2014-02-05-020, IJRETM, Vol: 02, Issue: 05, pp.1-7. Sep-2014

[7] Preneel, B. (2010, September). Cryptography for network security: failures, successes and challenges. In International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security (pp. 36-54). Springer, Berlin, Heidelberg.

[8] Stallings, W. (2006). Cryptography and Network Security, 4/E. Pearson Education India.