Cryptography in Network Security

S.T.Arokkiya Mary[1], S.Suganthi[2]
[1]Assistant Professor, Department of Computer Science, Bharathidasan govt. college for women, Puducherry.
[2] Assistant Professor, Department of Computer Science, Tagore Government Arts and Science College, Puducherry

Abstract: With the advent of the internet and the emergence of e-commerce applications and social networks, organizations across the world generate a large amount of data daily. Data security is the utmost critical issue in ensuring safe transmission of information through the internet. Network security is the security provided to a network from unauthorized access and risks. It is the duty of network administrators to adopt preventive measures to protect their networks from potential security threats. Network security is important for home networks as well as in the business world. Most homes with high-speed internet connections have one or more wireless routers, which could be exploited if not properly secured. A solid network security system helps reduce the risk of data loss, theft and sabotage. Computer security breaches are commonplace, and several occur around the world every day. Some are considered minor, with little loss of data or monetary resources, but many of them are considered major, or even catastrophic. Hackers are continuously looking for new vulnerabilities to exploit. When networks are not secured, information about organizations and individuals, and even our government are at risk of being exposed or leveraged against us. As the number of cyber-attacks increases, their knowledge and expertise are in growing demand. In this paper, an attempt has been made to review the various Network Security and Cryptographic concepts. This paper discusses the state of the art for a broad range of cryptographic algorithms that are used in networking applications.

Keywords: *e-commerce, network security, security threats, hackers, cryptography.*

I. Introduction

Computer security, cyber security [1] or information technology security (IT security) is the protection of computer systems from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide. The field is becoming more important due to increased reliance on computer systems, the Internet [2] and wireless network standards such as Bluetooth and Wi-Fi, and due to the growth of "smart" devices, including smart phones, televisions, and the various devices that constitute the "Internet of things". Due to its complexity, both in terms of politics and technology, cyber security is also one of the major challenges in the contemporary world [3]. Secure Network has now become a need of any organization. The security threats are increasing day by day and making high speed wired/wireless network and internet services, insecure and unreliable. Now-a-day's security measures works more importantly towards fulfilling the cutting edge demands of today's growing industries [4].

Network security [5] consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access.

II. Purpose Of The Study

A purpose statement of a security policy usually includes:

- Information regarding the preservation of ethical, legal, and security requirements.
- A security code of conduct for all to follow.
- Types of security policy practices being conducted..
- How a security policy provides a way to better outcomes – for each security policy.
- Types of security policy related plans.

III. Network Security

3.1 Model for Network Security

A model for much of what we will be discussing is captured, in very general terms, in Figure 1.5. A message is to be transferred from one party to another across some sort of internet. The two parties, who are the principals in this transaction, must cooperate for the exchange to take place. A logical information channel is established by defining a route through the internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the two principals.

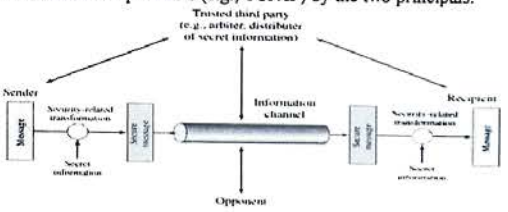

Figure 1: Model for Network Security

A message is to be transferred from one party to another across some sort of internet. The two parties, who are the principals in this transaction, must cooperate for the exchange to take place. A logical information channel is established by defining a route through the internet from source to destination and by the cooperative use of communication protocoB.ls (e.g., TCP/IP) by the two principals.

Using this model requires us to:

- design a suitable algorithm for the security transformation
- generate the secret information (keys) used by the algorithm
- develop methods to distribute and share the secret

ISBN: 978-93-5680-655-9

International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET

Optimized Weighted Trust Evaluation Based Intrusion Detection System in WSN

Dr. S. Suganthi

Assistant Professor, Department of Computer Science, Tagore Govt Arts and Science College, Puducherry, India

ARTICLEINFO

Article History:

Accepted: 05 April 2023
Published: 28 April 2023

Publication Issue
Volume 10, Issue 2
March-April-2023

Page Number
711-718

ABSTRACT

The individual nodes of a wireless sensor network (WSN) implemented in a hostile atmosphere might be readily penetrated by an adversary owing to restrictions such as short-term battery lifespan, storage capacity, and processing capabilities. It is vital to recognise and separate infected nodes with the goal to prevent being misled by the opponent's fake information provided through hacked nodes. However, due of their low flexibility and high communications cost, flat topological networks are difficult to protect effectively. In this research, we suggested an optimised based on weighted-trust assessment to identify malicious networks on top of hierarchy WSN architecture. In this study, we suggested an optimised weighted trust assessment-based intrusion detection system in WSNs, which makes use of a highly adaptable hierarchical trust administration method for clustering wireless sensor networks. To begin, a reliable assessment framework for trust perceptions is offered, which can calculate the node's trusted value based on its activity in order to successfully detect and isolate harmful nodes. Secondly, the trust evaluation model is introduced into an optimized path selection to increase security measures for data forwarding. The simulations of the outputs indicate that the suggested method greatly improves efficiency with respect to of packet loss percentage, end-to-end latency, efficiency, and use of energy, and also that it is resistant to black hole attacks.

Keywords: Wireless sensor networks, Optimized path selection, Weighted trust evaluation, Intrusion Detection, Sensor Node.

I. INTRODUCTION

As a result of the wide availability towards transmission, wireless sensor networks (WSNs) are now vulnerable to a range of assaults, including DoS incidents, manipulating attacks, sinkholes attacks, and so on. We explore putting up a matching system for intrusion detection around the outermost layer using edge computing to address the wireless sensor network

International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 04 | April - 2023 Impact Factor: 8.176 ISSN: 2582-3930

Business Opportunities, Mitigating and Managing Risks of the Prospective Entrepreneurs

S.Suganthi[1], S.T.Arokkiya Mary[2]

[1] Assistant Professor, Department of Computer Science, Tagore Govt. Arts and Science College, Puducherry, India
[2] Assistant Professor, Department of Computer Science, Bharathidasan Govt. College for Women, Puducherry, India

ABSTRACT

Entrepreneurship is critical to the expansion and development of any country's economy. Entrepreneurship functions as a preventative measure for a country's economic growth, resulting in the creation of job possibilities, national revenue, rural development, technical development, industrialization, export promotion, and so on. Entrepreneurs are the business's risk-takers. Risk management is key to operating any business in a profitable fashion. There are many risks facing an entrepreneur when starting and operating a new business venture. The trick is to eliminate risks that will hurt the venture, while taking on risks that will provide for long-term profitability. The risks facing the entrepreneur need to be initially identified as part of developing a business plan and revisited regularly in ongoing operations. Entrepreneurs transform ideas into economic possibilities via innovations, which are seen as a critical source of competitiveness in an increasingly globalizing world economy. The most significant problems are a shortage of funds, high raw material costs, and high loan rates. Most entrepreneurs had no prior business experience. Entrepreneurs judged finance, marketing, and company plan preparation to be the most valuable talents. 33% of hurdles are explained by firm age, size, and entrepreneur qualifications, implying that the younger and smaller the company, and the less qualified the entrepreneur, the more significant the problems.

Keywords: Business Opportunities, Entrepreneurs, Risk management, Mitigating and Managing Risks.

1. INTRODUCTION

Risk management is key to operating any business in a profitable fashion. There are many risks facing an entrepreneur when starting and operating a new business venture. The trick is to eliminate risks that will hurt the venture, while taking on risks that will provide for long-term profitability. The risks facing the entrepreneur need to be initially identified as part of developing a business plan and revisited regularly in ongoing operations [1]. Preparation for adverse events affecting a new business venture is necessary, but being too pessimistic or allowing fear of adverse events to stop an entrepreneur from taking any risk will keep a business venture from achieving it greatest potential and profit [2].

It is important that an entrepreneur develop an understanding of the risks of the business environment. The risks include liability risks stemming from contracts and torts, sometimes referred to as operating risks, regulatory compliance risks, financial risks, and strategic risks, including taxation [3]. Understanding how the business structure is used to operate the business venture allows the entrepreneur to develop a plan to manage business growth and understand business risk.

Human causes of risk refer to actions by employees, contractors, and those persons over which a company has control. These events can include torts stemming from negligence at work, labor strikes, shortages of qualified trained workers, and corporate mismanagement. An example of this type of risk would include embezzlement of money by an internal financial executive [4].

The use of a comprehensive approach allows a business entity to review and combine all risks into a functional perspective that allows the entrepreneur to evaluate risks and integrate new risks as different opportunities become more important to the business venture. Businesses sometimes use a risk matrix to assess or characterize the probability and impact of risk [5]. The use of such a tool can help a business quantify risk and decide whether to undertake an activity based on its level of risk.

  DOI: 10.55041/IJSREM20138