iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** VII **Month of publication:** July 2020

DOI: https://doi.org/10.22214/ijraset.2020.30449

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VII July 2020- Available at www.ijraset.com

A Survey on Cyber Security Threats and their Solutions

Sarfraz Nahid Hussain[1], Mr. N Rana Singha[2]
[1] *PG Student,* [2]*Assistant Professor, Department of Information Technology, Kaziranga University, Assam, India*

Abstract: ***Cyber attacks have increased nowadays in a rate which cannot be tackled through minimum security policies which we have for protecting our information inside the computer like creating passwords, PINs, installing anti-viruses to stop viruses and other threats that troubles our computer system or Firewalls for securing our information inside the network. With the rapid advancements in technology, hackers and other cyber criminals have opted to new modes through which they can steal important user information.***

To deal with such threats prone to our devices, we have made a survey on different types of cyber security attacks which are more common in today's scenario, their types and mode of attack and precautions that we can take to tackle such threats. We will study the tactics and measures adopted so far to tackle the problems created by these threats and make a comparative account on the different types of threats that are mostly effective in modern day context and their increase or decrease in the rate of prevalence per year.

Keywords: PINs, anti-viruses, Firewalls.

I. INTRODUCTION

A cyber security threat refers to an unauthorized or illegal activity that seeks to damage data, steal data, or disrupt personal digital information of a user in general. Cyber threats include computer viruses, data breaches, Denial of Service (DOS) attacks and other attack vectors.

Cyber security is the act of protecting computers, servers, mobile devices, electronic systems, networks and data from malicious attacks. With the rapid advancement in modern techniques in the field of computer networks and data sciences, it has become utmost important to derive new methodologies to secure private user or business information so that people other than the original user cannot get access to the data by any means. In the modern day scenario cyber security is the most researched area in information technology since cyber criminals or unauthorized users are adopting new techniques to trace and get access to important user information. So modern day security policies must be very effective so that these attackers or hackers do not easily get access to the important data of the user. For these several means of policies have been adopted like digital signatures and certificates but cyber security is such a field which must always be kept an eye on because these attackers are always searching for a way to breakdown or get access to the sensitive information of individual users and also the big companies illegally.

Vulnerabilities in cyber or computer security has been a major problem in today's scenario and it has always been considered as one of the deepest areas of research since a minor vulnerability can be utilized by the attackers to give rise to more devastating threats.

II. LITERATURE SURVEY

Cyber security has always been an area of deepest research for long. Cyber crimes have increased in a much higher rate due to advancement in technology to hijack data. We have discussed here in brief about some of the earlier proposed work. In Paper [1], the author speaks about the level of acceptance of the symmetric as well as asymmetric cryptography and how RSA algorithm has stood up to the level to which the authors were thinking that it would provide security. Paper [2] demonstrates on the different cyber forensic tools used in these days for detecting the identity of the criminals and accomplish law and security. Paper [3] mainly focuses on challenges faced by cyber security on the latest technologies .It also focuses on the major prerequisites of the cyber security techniques, ethics and the trends changing the face of cyber security. Paper [4] mainly focuses on the problems faced during processing of online bank transactions through credit cards. In paper [5] the author of this paper makes an analysis on the different threats that are posing problems in the different social networking sites in order to hijack personal information and modify them in order to defame the user in the society. The author researches and concentrate the cyber threats in social networking sites. They experienced the history of online social sites, classify their types and also discuss the cyber threats, propose the anti-threats methodologies and imagine the future patterns of such popular sites.

III. PROJECT OVERVIEW

In this project, we have made an comparative study of the most common threats that create trouble for our computer system and the network involved in sharing and transfer of information among various users. Some of the most common threats involved in capturing and modification of important user information that are used by hackers mostly are described below:

A. Viruses

A computer virus is a type of computer program that, when executed, replicates itself by modifying other computer programs and inserting its own code. When this replication succeeds, the affected areas are then said to be infected with a computer virus.

Computer viruses currently cause billions of dollars' worth of economic damage each year, due to causing system failure, wasting computer resources, corrupting data, increasing maintenance costs or stealing personal information. One of the ideal methods by which viruses spread is through emails opening the attachment in the email, visiting an infected website, clicking on an executable file, or viewing an infected advertisement can cause the virus to spread to your system. Besides that, infections also spread while connecting with already infected removable storage devices, such as USB drives. It is quite easy and simple for the viruses to sneak into a computer by dodging the defense systems. A successful breach can cause serious issues for the user such as infecting other resources or system software, modifying or deleting key functions or applications and copy/delete or encrypt data.

B. Trojan Horse

In computing, a Trojan horse, is any malware which misleads users of its true intent. It is a form of malware in which an attacker sends an email to the user computer that looks legitimate but can take control of the computer as soon as the user downloads it. Trojans may allow an attacker to access users' personal information such as banking information, passwords, or to the network. Ransomware attacks are often carried out using a Trojan.

A Trojan horse is not a single type of virus. It varies its purposes significantly. Cyber criminals or attackers can target the specific user or disseminate the Trojan horse of his choice anywhere he wishes.

C. Adware and Spyware

Adware, or advertising supported software, is software that displays unwanted advertisements on your computer. Adware programs will tend to serve you pop-up ads, can change your browser's homepage, add spyware and just bombard your device with advertisements. Adware is a more succinct name for potentially unwanted programs. It's not quite a virus and it may not be as obviously malicious as a lot of other problematic code floating around on the Internet. Make no mistake about it, though, that adware needs to come off of whatever machine it's on. Not only can adware be really bothersome every time you use your machine, it could also cause long-term issues for your device. Adware uses the browser to collect your web browsing history in order to 'target' advertisements that seem tailored to your interests. At their most innocuous, adware infections are just annoying. For example, adware barrages you with pop-up ads that can make your Internet experience markedly slower and more labour intensive.

As the name suggests, spyware is software that is designed to trace a user's data and forward it to cybercriminals or suspicious advertisement networks without their knowledge or consent. Such programs can sense the input entered by a user through the keyboard ('keyloggers'), collect confidential data (passwords, credit card numbers, pins, etc.), retrieve email addresses and can track everything the user types . Besides all this, spyware inevitably also affects the performance of the computer.

D. Man-in-the-middle Attack

A man-in-the-middle attack is a type of cyber attack where a criminal introduces himself into conversation between two parties, impersonates both parties and gains access to their personal information which by no means be disclosed. It allows a malicious actor to intercept, send and receive data meant for someone else without the knowledge of the parties that are actually communicating.

Below given example clearly illustrates the MITM attack and how a third party comes into action and steals the data transferred during the communication between two individuals:

The attacker is impersonating both sides of the conversation to gain access to funds. This example demonstrates the hijacking of information in a conversation with a client and a server as well as person-to-person conversations. In this example, the attacker intercepts a public key that can transpose his own data to trick the people on either end into believing that they are communicating with one another securely.

Though MITM attacks can be protected against with encryption, professional cyber criminals can either re-route traffic to phishing sites designed to look legitimate or simply pass on traffic to its intended destination once recorded, thus detection of such attacks are utmost difficult.

E. Computer Worms

A computer worm is a type of malicious software program whose primary function is to infect other computers while remaining active on infected systems. A computer worm is self-replicating malware that duplicates itself to spread to uninfected computers. Worms often use parts of an operating system that are automatic and invisible to the user. It is common for worms to be noticed only when their uncontrolled replication consumes system resources, slowing or halting other task.

A computer worm infection spreads without user interaction. All that is necessary is for the computer worm to become active on an infected system. Before widespread use of networks, computer worms were spread through infected storage media, such as floppy diskettes, which, when mounted on a system, would infect other storage devices connected to the victim system. USB drives are still a common vector for computer worms.

F. DOS and DDOS attacks

A DoS attack tries to make a web resource unavailable to its users by flooding the target URL with more requests than the server can handle. That means that during the attack period, regular traffic on the website will be either slowed down or completely interrupted.

A Distributed Denial of Service (DDoS) attack is a DoS attack that comes from more than one source at the same time. A DDoS attack is typically generated using thousands (potentially hundreds of thousands) of unsuspecting zombie machines. The machines used in such attacks are collectively known as “botnets” and will have previously been infected with malicious software, so they can be remotely controlled by the attacker. According to research, tens of millions of computers are likely to be infected with botnet programs worldwide.

Cybercriminals use DoS attacks to extort money from companies that rely on their websites being accessible. But there have also been examples of legitimate businesses having paid underground elements of the Internet to help them cripple rival websites. In addition, cybercriminals combine DoS attacks and phishing to target online bank customers. They use a DoS attack to take down the bank's website and then send out phishing e-mails to direct customers to a fake emergency site instead.

In todays scenario, DoS attacks have proven to be very profitable and are taking over the Internet. The Network Infrastructure Security Report points out that DDoS attacks have increased by 1000 per cent since 2005. 2010's biggest attack doubled in scale compared to 2009, with one attack in particular bombarding its target at 100 gigabits per second.

IV. RESULTS AND DISSCUSSIONS

We are living in a society which is hugely dependent on computer networks and evolved internet technology. So, it has become a matter of utmost concern that our data and information that we are sharing through internet is protected and secured and none other than us has access to the information. We should only be the one to get access to modify or view any changes in the data we saved earlier and no other person by any mean can retrieve or manipulate the data. In this regard cyber security has become a great issue for the modern generation which hugely rely on the internet for their useful works and also for companies who depend on internet for their business purposes to make contact between their different employees and share business related data. In the modern scenario, cyber security has always been an important area of research for most of the research scholars as well as cyber security analysts since it has always been considered important to search for new technologies and advancements in this field so that hackers and attackers by any means get a way to steal the valuable information which should not be disclosed to others.

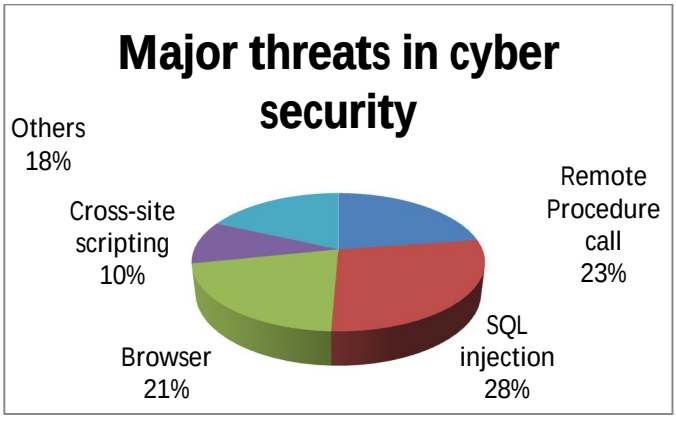


Fig. -1 : Graphical representation of major cyber security threats

A. Exploitation Of Existing Vulnerabilities In The System And Network

As soon as cybercriminals send the malware into the victim's computer through the infected software or websites, they can make use of the vulnerabilities present in the network and manipulate their actions accordingly. We will discuss on some of the common hardware, software and network vulnerabilities and some tactics imposed so far to deal with such malicious efforts of attackers.

1) *Hardware Defects:* Hardware is the most privileged entity and has the most ability to manipulate a computing system. If the hardware configuration is compromised attackers get considerable flexibility and power to launch malicious security attacks Compared to software level attacks where many security patches, intrusion detection tools, and anti-virus scanners exist to detect malicious attacks periodically, many of the hardware-based attacks do not get recognized. Taking advantage in lack of tools to detect intrusion in hardware, the hardware-based attacks have been reported to be more frequent than software and network attacks. Among different types of hardware misuse, hardware Trojan is the most effective and common hardware exploits. The hardware Trojans are malicious and deliberately unnoticeable modification made to electronic devices such as Integrity Circuits (IC) in the hardware. The hardware Trojans have a variety of degrees which can create different types of undesirable effects. A hardware Trojan might cause an error detection module to accept inputs that should be rejected. A Trojan might insert more buffers in the chip's interconnections and hence consume more power, which in turn could drain the battery quickly. In more serious case, Denial-of-Service (DoS) Trojans prevent operation of a function or resource that perform a specific task for the system. A DoS Trojan can cause the target module to exhaust scarce resources like bandwidth, computation, and battery power. It could also physically destroy, disable, or alter the device's configuration. The chance to produce unauthentic hardware has increased with a new trend in IT companies trying to reduce their IT expense via out sourcing and buying of fun trusted hardware from online sites..Similarly, it is also pointed out that IT companies often buy untrusted hardware such as chip sets and routers from online auction sites or sellers which in turn may contain harmful hardware-based Trojans. These practices are not only problematic for IT com-panies operated on the tampered hardware with potential back door entry, it also increases the chance that the original design and the details of internal states of system to be leaked to unauthorized personnel.

Table -1 : Countries with their increase in percentage of cyber attacks per year (From 2017)

1	U.S.A	90.8
2	Australia	88.0
3	Japan	88.0
4	Singapore	87.7
5	South Korea	86.8
6	New Zealand	82.0
7	Malaysia	73.2
8	China	70.2
9	Taiwan	56.9
10	India	55.8

2) *Software Defects:* A software bug is the common term used to describe an error, flaw, mistake, or fault in a computer program such as internal OS, external I/O interface drivers, and applications Cyber attacks utilize the software bugs in their benefits to cause the systems to behave unintended ways that are different from their original intent. The majority of cyber attacks today still occur as a result of exploiting software vulnerabilities caused by software bug and design flaws Software based exploitation occurs when certain features of software stack and interface is exploited. Most common software vulnerabilities happen as a result of exploiting software bugs in the memory, user input validation, race conditions and user access privileges Memory safety violations are performed by attackers to modify the contents of a memory location. Most exemplary technique is buffer overflow. The buffer overflow occurs when a program tries to store more data in a buffer than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. It allows attackers to interfere into existing process code. Input validation is the process of ensuring that the input data follows certain rules. Incorrect data validation can lead to data corruption such as in SQL injection. SQL injection is one of the most well known techniques that exploit a program bug in a website's software. An attacker injects SQL commands from the web form either to change the database content or dump the database information like

credit cards or passwords to the attacker. Adversary exploits a flaw in a process where the output of the process is unexpectedly and critically dependent on the timing of other events. The time of check to time of use is a bug caused by changes in a system between the checking of a condition and the use of the results of that check. It is also called exploiting race condition error. Privilege confusion is an act of exploiting a bug by gaining elevated access to resources that are normally protected from an application or user. The result is that adversaries with more privileges perform unauthorized actions such as accessing protected secret keys.

3) *Network Infrastructure and Protocol Vulnerabilities:* The early network protocol was developed to support a completely different environment that we have today and in a much smaller scale, and often does not work properly in many situations it is used today. Weaknesses in network protocols are of immense effect when both system administrators and users have limited knowledge of the networking infrastructure For example, in cases where the system administrators do not use efficient encryption scheme, do not apply recommended patches on time, or forget to apply security filters or policies network security becomes a headache for both sides. One of the most common network attacks occurs by exploiting the limitations of the commonly used network protocols Internet Protocol (IP), Transmission Control Protocol (TCP) or Domain Name System (DNS). The IP is the main protocol of the network layer. It provides the information needed for routing packets among routers and computers of the network. The original IP protocol did not have any mechanism to check the authenticity and privacy of data being transmitted. This allowed the data being intercepted or changed while they are transmitted over unknown network between two devices. To prevent the problem, IPSec was developed to provide encryption of IP traffic. In many years, IPSec has been used as one of the main technology for the creation of a virtual private network (VPN) which creates a secure channel across the Internet between a remote computer and a trusted network (i.e company intranet). TCP sits on top of the IP to transmit the packets in reliable (i.e retransmitting lost packets) and ordered delivery of the packets .SSL was originally developed to provide end-to-end security, as oppose to only layer based protocol, between two computers which sits over the transmission control protocol (TCP). SSL / TLS is commonly used with http to form https for secure Web pages. The domain name server (DNS) is the protocol that translates the human-readable host names into 32 bit Internet protocol (IP) addresses. It is essentially works as a directory book for the Internet telling routers to which IP address to direct packets when the user gives a url. Because DNS replies are not authenticated, an attacker may be able to send malicious DNS messages to impersonate an Internet server. Another concern about DNS is its availability. Because a successful attack against the DNS service would create a significant communication disruption in the Internet, DNS has been the target of several Denial-of-Service (DoS) attacks.

Table -2 : Total no. of attacks occurred from Jan-June 2012 to Jan-June 2013

Incident	Jan-Jun 2012	Jan-Jun 2013	% increase decrease
Fraud	2439	2490	2
Intrusion	2203	1726	22
Spam	291	614	111
Malicious code	353	442	25
Cyber harassment	173	233	35
Content related	10	42	320
Intrusion attempts	55	24	56
Denial of services	12	10	17
Vulnerability reports	45	11	76
Total	5581	5592	

V. CONCLUSIONS

In this project, we have made a general survey on some of the common threats which can cause defects in the communication and information sharing between different computers connected within a network. We have also studied the mechanism of propagation and defect caused by such threats and what strategies can be adopted by the different corporate companies as well as banks to provide adequate security to their users.

We have studied one basic type of cyber attack called Man-in-the-middle attack or MITM attack which have been considered as one of the major threats in cyber security nowadays. We have studied the mode of performing such attacks and how attackers have used it to steal important user information to cause huge losses in business or other monetary transactions. We have also made a comparative study on the various types of attacks or threats studied by us in the present context of the world and strategies taken by different countries to tackle such cyber attacks.

VI. ACKNOWLEDGEMENT

We would like to express our heartiest thanks with a deep sense of gratitude and respect to all those who provided us immense help and guidance during the completion of this project.

We would like to thank our project guide Mr. N Rana Singha for providing us immense help and support and guiding us about the carrying out of the different activities. We have been greatly benefited from his regular critical reviews and inspiration throughout our work. Last but not the least we would like to mention here that we are greatly indebted to each and everyone who has been associated with our project at any stage but whose name does not find a place in this acknowledgement.

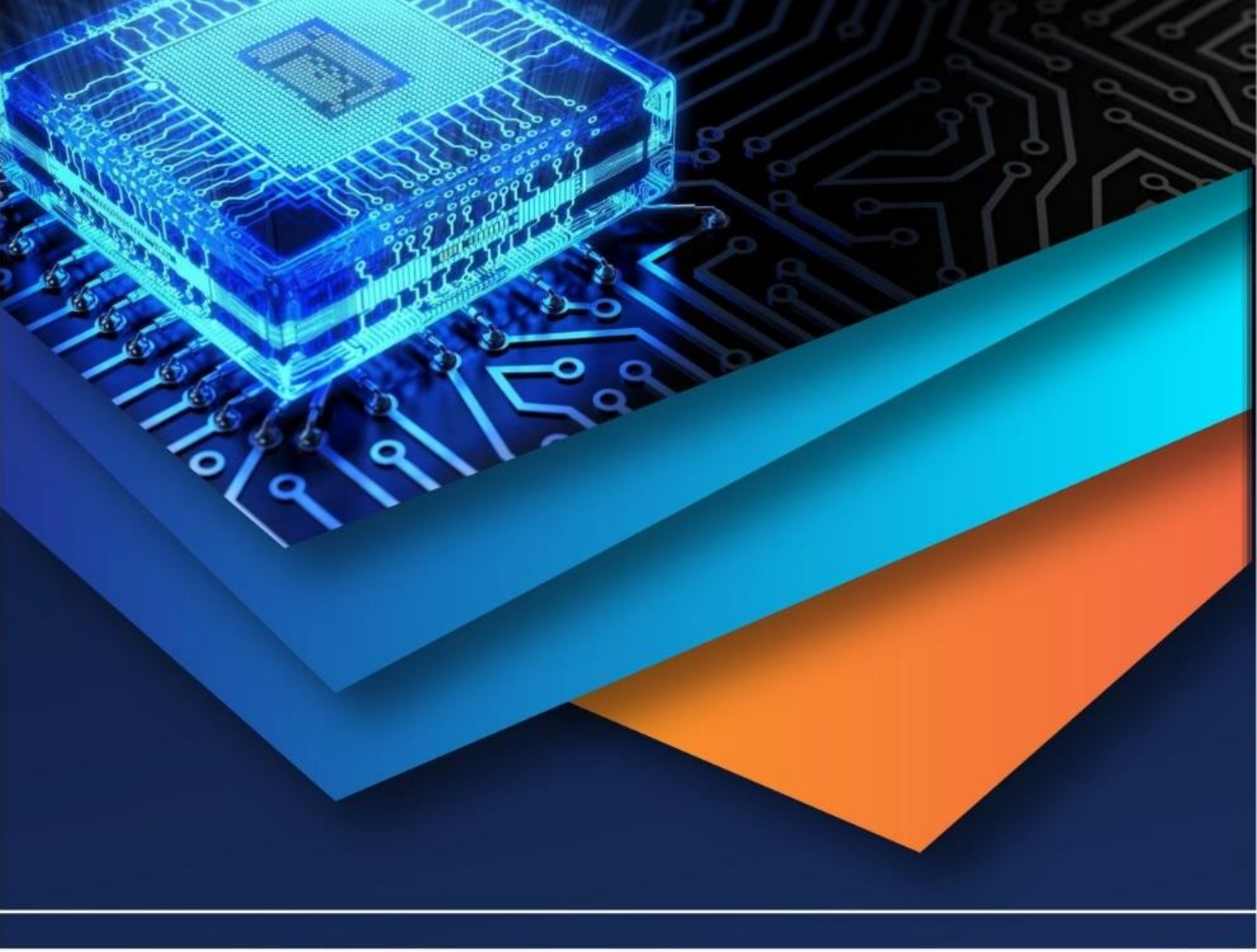
REFERENCES

[1] Rohit Minni, Kaushal Sultania, Saurabh Mishra, Prof Durai Raj, etal , "An Algorithm to Enhance security in RSA" ICCNT.2013.6726517
[2] Raza Hasan, Salman Mahmood, Akshyadeep Raghav School of Computing, "Overview on Computer Forensics Tools" CONTROL.2012.633466
[3] G.Nikhita Reddy, G.J.Ugander Reddy, etal. "A Study of cyber security challenges and its emerging trends on latest technologies" Published in ArXiv 2014 Corpus ID: 6758838
[4] K. RamaKalyani, D.UmaDevi Department, etal, "Fraud Detection of Credit Card Payment System by Genetic Algorithm" ISSN 2229-5518
[5] Dr. Sunil Kumar, Vikas Somani, etal. "Social Media Security Risks, Cyber Threats And Risks Prevention And Mitigation Techniques" article in IJAR in Computer Science and Management, May 2018
[6] Sonu B. Surati, Ghanshyam I. Prajapati, etal, "A Review on Ransomware Detection & Prevention" IJRS, Volume IV, Issue IX, September 2017, ISSN 2321-2705

BIOGRAPHIES

PG Student, pursuing Master's degree in IT, Kaziranga University. Possesses good skills in MS Office, Programming in Python and Amazon AWS.

Assistant Professor, IT, Kaziranga University. Completed B.Tech in Computer Science from NIT Silchar and M.Tech in IT from Tezpur University.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY