Scientific Research Publishing

Journal of Information Security, 2021, 12, 56-78
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Cyber Security Crimes, Ethics and a Suggested Algorithm to Overcome Cyber-Physical Systems Problems (CybSec1)

Abou_el_ela Abdou Hussien

Computer Science Department, Modern Academy-Maddi, ARE, Maddi, Egypt
Email: abo_el_ela_2004@yahoo.com

How to cite this paper: Hussien, A.A. (2021) Cyber Security Crimes, Ethics and a Suggested Algorithm to Overcome Cyber-Physical Systems Problems (CybSec1). *Journal of Information Security*, **12**, 56-78.
https://doi.org/10.4236/jis.2021.121003

Received: November 30, 2020
Accepted: January 12, 2021
Published: January 15, 2021

Abstract

Digital systems have changed our world and will continue to change it. Supportive government policy, a strong research base and history of industrial success place the benefits of an emerging digital society. Protecting benefits and minimizing risks requires reliable and robust cyber security, backed by a robust research and translation system. Trust is essential for growth and maintenance of participation in the digital community. Organizations gain trust by acting in a trustworthy way leading to building reliable and secure systems, treating people, their privacy and their data with respect, and providing reliable and understandable information to help people understand how safe they are. Research and revolution in industry and academia will continue to make important contributions to create flexible and reliable digital environment. Cyber Security has a main role in the field of information technology because securing information has become one of the greatest challenges today. When we think about the cyber security, the first thing that comes to our mind is "cyber crimes" which are increasing exponentially day by day. Many governments and firms are taking many measures to prevent these cybercrimes. Besides the various measures, cyber security remains a major concern. This paper intended to give a deep overview of the concepts and principles of cyber security that affect the safety and security in an international context. It mainly focuses on challenges faced by cyber security on the latest technologies and focuses also on introducing security types, cyber security techniques, cyber security ethics, trends that change the face of cyber security and finally attempting to solve one of the most serious cyber security crimes of violating privacy on the internet by improving the security of sensitive personal information (SPI) in Cyber-physical systems using a selected proposed algorithm that analyzes the user's information resources and determines the valid data to be encrypted, then uses adaptive acquisition me-

thods to collect the information and finally a new cryptographic method is used to complete SPI secure encryption according to acquisition results as described in details in Section 4.

Keywords

Cyber Security, Cybercrime, Cyber Ethics, Social Media, Cloud Computing, Android Apps

1. Introduction

Today a person can send and receive any form of data that may be an e-mail, voice or video with just one click of a button, but has he ever thought about how safe it is to send his data ID or send it to the other person safely without any leakage of information? The answer could be found in cyber security. Today the Internet is the fastest growing infrastructure in everyday life. In current technical environment, many modern technologies are changing the face of humanity. But due to these emerging technologies, we are not able to protect our private information in a very effective way and hence these days' cybercrime is increasing day by day. Today more than 60 percent of all commercial transactions take place over the internet, so this field requires a high quality of security for transparent transactions and best transactions. Hence cyber security becomes a recent issue. The scope of cyber security is not only limited to securing the information in the IT industry, but also includes many other areas such as cyberspace etc. Even the latest technologies like cloud computing, mobile computing, E-commerce, internet banking, etc. need a lot of security. Since these technologies contain some important information regarding a person, it has safely become a must. Strengthening cyber security and protecting critical information infrastructures is essential to every nation's security and economic well-being. Making the Internet safer (and protecting Internet users) has become an integral part of developing new services as well as government policy. Many countries and governments today enforce strict laws on electronic securities in order to prevent the loss of some important information. Everyone must also be trained on this cyber security and save themselves from these increasing cybercrimes [1]. However, are we aware and prepared enough as individuals, nations or the international community of the threats coming from cyberspace or to deny the use of this dimension of communication, trade and even war? Namely, despite the increasing number of users, the Internet is still outside or below the minimum level of regulation. There are security problems in cyberspace that represent a threat and challenge in the modern era. The development and application of information and communications technologies have created a new battlefield. As a special challenge to international security, cyber terrorism is emerging, and cyber security will greatly affect international relations in the twenty-first century.

Here we try to solve one of the most serious cyber security crimes of violating privacy on the internet by enhancing the security of sensitive personal information (SPI) in Cyber-physical systems using a selected proposed algorithm. Section 2 discuss related topics with cyber security as cybercrime, cyber security risks, security types, security problems, types of hackers, and Advantages and disadvantages of cyber security. Section 3 introduces cybercrime history and types, cyber security techniques and ethics, and best practices to overcome cyber security risks. Section 4 introduces problem that faces sensitive information security and proposed algorithm to solve it.

2. Related Topics

2.1. Cybercrime

Cybercrime is a term that refers to any illegal activity that uses computers as the primary method for commission and theft [1]. The U.S. Department of Justice is expanding the definition of cybercrime to include any illegal activity that uses a computer to store evidence. The growing list of cybercrimes includes crimes made possible by computers, such as breaking into networks and spreading computer viruses, as well as computer forms of existing crimes, such as identity theft, stalking, bullying and terrorism that have become a major problem for people and nations. cybercrime is usually defined in common man's language as a crime committed by using computer and the internet to steal a person's identity, sell contraband, stalk victims or disrupt operations with malicious software. As technology plays a major role in a person's life, cybercrimes will also increase along with technological advancements.

2.2. Trends Changing Cyber Security

Here are some of the trends that have a major impact on cyber security [1].

- **Web Servers**

The warning of attacks on web applications to extract deduction or to distribute malicious code continues. Cyber criminals distribute their malicious code via the legitimate web servers that they hacked. But data theft attacks, many of which attract media attention, also pose a significant threat [1]. Now, we need a greater focus on protecting web servers and web applications. Web servers in particular are the best platform for these data-stealing cyber criminals. Consequently one must always use a secure browser especially during dominant transactions in order not to fall prey to these crimes.

- **Cloud Computing and Its Services**

These days, all small, medium and large businesses are slowly adopting cloud services [1]. In other words, the world is slowly moving towards clouds. This latest trend presents a major challenge to cyber security, as traffic can revolve around traditional checkpoints. Additionally, as the number of applications available in the cloud grows, policy controls for cloud facilities and web users will also need to develop in order to prevent the loss of important information.

Even though cloud services have developed their own models, a lot of issues still arise about their security. The cloud may offer enormous opportunities, but it should always be noted that as the cloud develops so as its security interest's increase.

- **APT's and Targeted Attacks**

APT (Advanced Persistent Threat) is a whole new level of cybercrime tool. For many years, network security capabilities such as web filtering or IPS have played a major role in identifying such targeted attacks (often after the initial hack) [1]. As attackers become more daring and use more obscure technologies, network security must integrate with other security services in order to detect attacks. One must improve our security technologies to prevent more coming threats in the future.

- **Mobile Networks**

Today we are able to contact anyone in any part of the world. But for these mobile networks, security is a very big concern [1]. Firewalls and other security measures these days have become porous as people use devices like tablets, phones, computers, etc. all of which again require additional securities apart other than the ones in the applications used. We should always care about the security issues of these mobile networks. More mobile networks are highly vulnerable to this cybercrimes and great care must be taken if there are security issues with them.

- **IPv6: New Internet Protocol**

IPv6 is the new Internet protocol that replaces IPv4 (the older version), which was the backbone of networks in general and the Internet at large [1]. Protecting IPv6 is not just a matter of transferring IPv4 capabilities. While IPv6 is a wholesale alternative in making more IP addresses available, there are some very basic changes to the protocol that must be taken into account in the security policy. Hence it is always better to switch to IPv6 as soon as possible to reduce the risks related to cybercrime.

- **Encryption of the Code**

Encryption is the process of encoding messages (or information) in a way that an intruder or hackers cannot read [1]. In a cipher system, a message or information is encrypted using an encryption algorithm, which turns it into unreadable cipher text. This is usually done with an encryption key, which specifies how the message is encrypted. Encryption initially protects data privacy and its integrity. But more use of cryptography brings more challenges in the field of cyber security. Encryption is also used to protect data during transmission, for example data that is transferred over networks (as the Internet, e-commerce), mobile telephones, wireless micro-phones, wireless intercoms etc. Hence through the code encrypting, it can know if there is any information leakage. The top network threats are explained in **Figure 1**.

2.3. Cyber-Attack

Whether it occurs as an interstate conflict between states, terrorist or a criminal

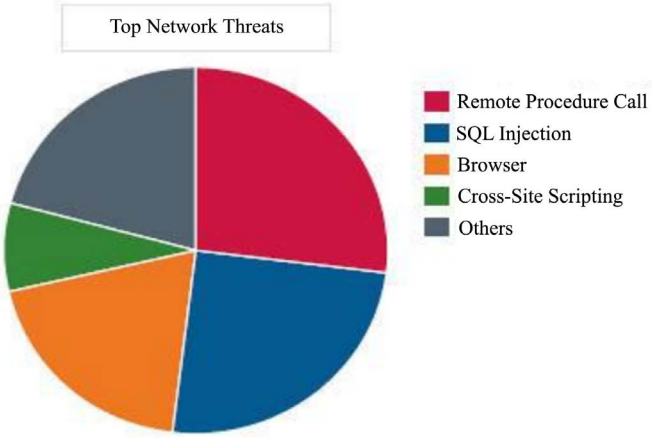

Figure 1. Pie chart shows about the major threats for networks and cyber security.

act, it is an attack in cyberspace with the aim of endangering a computer system or network, but also damaging physical systems as was the case with the Stuxnet worm [2]. In layman's common terminology, which is often mentioned in the media, it is called a hacker attack. Identical hacker attack methods are applied for both military and terrorist purposes. Janczewski and Colarik [3] divided cyber-attacks into phases, which they consider to be basically the same as the phases of conventional criminal offenses:

1) The first phase of the attack is to uncover potential victims. By monitoring the implementation of the target's normal operations, and useful information that is gathered and identified by the applications and devices used;

2) The second phase of the attack is the storming. Until the attacker enters the system, there is not much that can be done against the target except for disrupting availability or accessing specific services provided by the target;

3) The third phase is to identify and deploy internal opportunities by examining the resources and the right to access restricted and important parts of the system;

4) In the fourth phase, the intruder destroys the system or steals certain data; Moreover they point out that today's cyber-attacks consist mainly of:

- Malignant software via attachments in the Internet browser, e-mail or other system vulnerabilities;
- Denial of service (DoS) to prevent the use of computer systems and networks;
- Deletion or transfer (leaving a message) to government and commercial sites for advertising purposes or to disable the media;
- Unauthorized intrusion into systems to steal confidential and/or private Information, compromise data or use the system to launch attacks.

In such circumstances of transformation and different perspectives and understandings of security in general and international security, cyber threats are definitely redefining these terms. In line with the efforts made to ensure security on the one hand and the peculiarities of cyber threats and the motives of the actors who started them on the other hand, it will be necessary to create a new in-

ternational security paradigm for the cyber age.

2.4. What Are the Cyber Security Risks While Working Remotely?

Let us quickly take a look at some of the potential threats you may face while working remotely [4]:

- There is no physical security
- Communication gap
- Concurrent VPN connections are not supported
- Lack of appropriate access, authorization, documentation policies for implementation
- Poor data backup implementation
- Disk encryption for endpoints
- Wi-Fi connections are not secure
- Easy logins and passwords

2.5. Counter Measures

Could be defined as the actions that could be taken to secure applications [5]. The primary program for countermeasure is **application firewall** that secures files or data processing by specific installed software. The most familiar hardware countermeasure is **a router** that can save the IP addresses of a single computer system to be visible directly on the internet.

Other countermeasures include:

- Traditional firewalls,
- programs or algorithms for encryption or decryption processes,
- anti-virus programs, spyware detection and removal programs,
- Biometric authentication systems.

2.6. Security Types

1) Communication Security: Communication security is also known as COMSEC [5]. COMSEC is a process of securing or preventing unauthorized access to the traffic that will be generated from communication systems, or it will also assist with any written information that is sent or transferred to another device via any other means. There are several COMSEC disciplines, including [5]:

- **Cryptographic Security:** It encrypts the data on the sender side and makes it unreadable until the data is decrypted by receiver side.
- **Emission Security:** Used to prevent the release or capture emission of equipment to prevent information from unauthorized interception.
- **Physical Security:** It ensures by preventing unauthorized access to encryption information, documents and equipment on the network.
- **Transmission Security:** It is used to protect unauthorized access when data is physically transferred from one side to another or one medium to another to prevent issues such as service interruption, data theft by a malicious per-

son.

- **Security Information Security:** Used to protect information or data and its crucial elements, including systems program and hardware that are used to store or transmit that information. Information security is also known as Infosec. Infosec is a set of strategies for managing processes and tools used in software and program policies that are primarily for security purpose and are necessary to prevent, detect and combat threats to digital and non-digital information [5].

Infosec responsibilities include a set of business processes that will protect the information assets of how information is formatted, whether or not it is transmitted, processed, or in a storage state. Infosec programs follow the basic objectives of CIA confidentiality, integrity and availability: they maintain confidentiality and ensure that sensitive information is not disclosed except to authorized parties, and integrity stands to prevent unauthorized modification of data and availability that guarantees access to data by authorized parties when request IT systems and business data.

2) Network Security: Network security is used to protect network components, network connectivity and network-related content [5]. A network security system is typically based on layers of security and consists of more than one component that is included in a network to monitor network and security software and hardware devices, and its appliances. All components work together to increase the security and overall performance of your computer network.

3) Operational Security: Operational security is an analytical process that categorizes information assets and specifies the controls required to secure these assets. Operational security is also known as OPSEC. Operational security typically consists of iterative process of five-step [5]:

- **Identify Critical Information:** The first step is to find out what data may particularly affect the organization or be harmful to the enterprise if obtained by the opponent. This includes intellectual property and/or personal information and financial data for employees and/or clients.
- **Identify Threats:** The next step is to identify the code or program that poses a threat to the organization's private or sensitive information. There may be many antagonists targeting different pieces of information, and companies should consider any competitors or hackers that might be targeting the data.
- **Vulnerability Analysis:** In the vulnerability analysis stage, the organization examines potential weaknesses among the safeguards in place to protect the private information that makes it vulnerable to potential adversaries [6]. This step includes identifying any potential vulnerability in physical/electronic operations designed to protect against predefined threats, or areas where lack of security awareness training leaves information Vulnerable to attack.
- **Risk Assessment:** After identifying the vulnerabilities, the next step is to find the threat level associated with each. Companies classify risks according to factors such as the likelihood that a specific attack will occur and extent to which such an attack damages operations. The higher the risk, the greater the

urgency for the organization to implement risk management controls.

- **Implement Appropriate Countermeasures:** The final step is to implement a risk mitigation plan starting with those that pose the greatest threat to operations. Potential security improvements arising from the risk mitigation plan include implementing additional hardware and training or developing new information management policies.

2.7. Problematic Elements of Cyber Security

One of the most problematic elements of cyber security expert who may security is the security risks [5]. The traditional approach focused most of the resources on the most important system components and protection from threats, which necessitated leaving some of the less important components of the system without protection and some of the less serious risks, *i.e.* unprotected. Such an approach is inadequate in the present medium.

2.8. Major Security Problems

- **Virus:** Virus is a program that you download onto your computer without your knowledge and that works against your wishes [5]. These are computer programs that attach themselves or infect a system or files, and tend to spread to other computers on the network by clicking on them, through mail, through external devices, etc. They disrupt the operation of the computer and affect the data stored either by modifying or completely removing them. Example of viruses: (1) Conficker, (2) Stuxnet, (3) Mydoom (4) Melissa, (5) Sasser, (6) Zeus, (7) Code Red.
- **Warms:** Worms unlike viruses do not need a host to hang on. It only multiplies until it is complete eats up all current memory in the system [5]. The term worm is sometimes used to refer to self-replicating malware (MALicious softWARE). It occupies some free memory from external devices or drives. An example of warms: (1) Blaster, (2) ExploreZip, (3) Badtrans, (4) Bagle, (5) Kak worm, (6) Supernova Worm, (7) Netsky, (8) SQL Slammer.
- **Hacker:** In general, a hacker is someone who breaks into computers, usually by accessing administrative controls.

2.9. Types of Hackers

1) White Hat Hacker: A white hat hacker is a computer security professional person who penetrates into secure systems and networks to examine and evaluate their security [5]. The white hat hacker uses his skills to improve security by exposing vulnerabilities before malicious hackers (known as black hat hackers) can discover and exploit them. Although the methods used are similar, if not identical, to those used by malicious hackers, the white hat hackers have permission to employ it against the organization that has hired them.

2) Grey Hat Hacker: The term "grey hat" or "gray hat" refers to a computer hacker or computer security expert who may occasionally violate laws or exemplary ethical standards, but has no malicious intent as is the case with a black hat

hacker [5].

3) Black Hat Hacker: A black hat hacker is a person who has extensive computer knowledge and is intended to hack or bypass internet security [5]. Black hat hackers are also referred to as crackers or dark side hackers. The general opinion is that while hackers build things, crackers break things.

- Malware: refers to the term "MALicious software". Without the knowledge or allowance of the system owner Malware program affects and damages the computer system. a) Spyware, b) Crime ware, c) Adware d) Viruses, e) Warms, f) Root kits, g) Trojans.
- Trojan horses: Trojan horses are email viruses that can copy themselves, theft information, or damage the computer system. These viruses are the most dangerous threats to computers.
- Password Cracking: are attacks by hackers that are able to decide passwords or find passwords to different protected electronic areas and social network sites.

2.10. Management of Cyber Security Risks

Three factors affect the risk associated with any attack: the threats (who attacks), vulnerabilities (the lack they attack), and impacts (what the attack does). Managing risks to information systems is fundamental to effective cyber security [7]. What are the threats? People who actually carry out cyber-attacks are widely referred to as falling into one or more of five categories: criminals who intend to achieve financial gain from crimes such as theft, extortion, or corrupting the system spies, with the intent to steal confidential or government-owned or private information; nation-state fighters who develop their capabilities and conduct cyber-attacks in support of the strategic goals of states; activists who carry out cyber-attacks for non-financial reasons; and terrorists who participate in cyber-attacks as a form of non-state or state-sponsored warfare.

What are the Vulnerabilities? In many ways, Cyber security offensive race between attackers and defenders. ICT systems are extremely complex, and attackers are constantly looking for Vulnerabilities that can occur at many points. Defenders can often protect against Vulnerabilities, but there are challenges in particular: unintended or intentional actions by insiders who have access to a system; supply chain weaknesses, which could allow malicious software or hardware to be introduced during the procurement process; and previously unknown vulnerabilities with no established fix. Even for weaknesses where treatments are known, they may not be implemented due to budgetary or operational constraints. A network administrator would use these types of programs by trying that if an attacker could easily attack the database or not? Is there any vulnerability that harms program security or database security? Whereas, a hacker would use these types of vulnerable programs to breach user details [6].

What are the effects? A successful attack could harm the confidentiality, integrity, and availability of an ICT system that deals with it. Cyber theft or cyber espionage can filter financial, private, or personal information that the attacker

can take advantage of, often without the victim knowledge [8]. Denial-of-service attacks can slow or prevent legitimate users from accessing the system. Botnet malware can give an attacker command of a system to use for cyber-attacks on other systems.

2.11. Advantages and Disadvantages of Cyber Security

We introduce here some of advantages and disadvantages of cyber security [5]:

- **Advantages of Cyber Security**

1) Improving cyberspace security.
2) Increasing cyber defense.
3) Increasing the internet speed.
4) Protecting data and information for companies.
5) Systems protecting from viruses, worms, malware, spyware, etc.
6) Protecting personal privacy.
7) Protecting networks and data and storage resources.
8) Fighting hackers and identity theft for computer system
9) Reduces computer freezes and crashes.
10) It gives privacy preserving of users.

- **Disadvantages of Cyber Security**

1) It will be expensive for regular users.
2) It can be difficult to properly configure firewalls.
3) Need to update to the new software in order to keep security up to date.
4) Slower the system than before.
5) Incorrectly configured firewalls may prevent users from performing certain actions on the Internet, until the firewall is properly configured.

2.12. Safety Tips for Cyber Security

1) Use antivirus program.
2) Insert firewalls, pop up blocker.
3) Delete unnecessary software.
4) Keep Maintaining backup.
5) Examine security settings.
6) Keep connection secure.
7) Be careful when opening attachments.
8) Strong passwords must use (keep combination of uppercase, lowercase, special characters etc.).
9) Do not give personal information unless required.

3. Issues in Cyber Security

1) Better end-user education is a bit of an expression of intuition, but most frameworks are just as safe as the tendencies of the general public who use them. Horrible screen characters abuse this to exploit weak passwords, uncorrected scripting, and use complex phishing strategies [9].

2) Development of security-conscious programming: They are not individuals who focus on security. With more people connecting to the internet, so do the security risks that pose more risks to harm information, programming, and tools as well.

3.1. Cybercrime

Cyber security is needed when carrying out a crime: previous descriptions were "computer crime", "computer-related crime" or "crime by computer" [5]. With the spread of digital technology, some new terms such as the crime of "high-technology" or "information age" have been added to the definition [6]. The Internet has also brought in other new terms, such as "cybercrime" and "net crime". There are other forms of crimes include "digital", "electronic", and "virtual" crime, "Information Technology", "high-technology" and "enabling technology". It will do this through people who mostly connect to internet, online activities, social activities, etc.

3.1.1. History of Cybercrime

1) The year 1820 recorded the first cybercrime.

2) The first spam email took place in1978 when it was sent over the Arpanet.

3) Apple Computer in 1982 recorded the first Virus was installation.

3.1.2. Types of Cybercrime

There are 12 types of cybercrimes as follows [5]:

1) Hacking

Hacking is an act that is done by an intruder by gaining access to your computer system without your permission [5]. Hackers (the people who do hacking) are basically computer programmers, who have an advanced understanding of computers and usually misuse this knowledge for deceptive reasons:

a) SQL injections

b) FTP passwords theft

c) Via site programming

2) Virus Spread

Viruses are computer programs that bind to or infect a system or files, and have a tendency to spread to other computers on the network [5]. They disrupt the operation of the computer and affect the stored data by either modifying or deleting it completely.

3) Logic Bombs

A logic bomb, also known as slag code, a malicious code, piece of code that is intentionally inserted into a program to perform a malicious task when triggered by a specific event [5].

4) Denial-of-Service Attack

A Denial-of-Service (DoS) attack is a precise try by attackers to prevent service to intend users of that service [5]. It involves flooding the computer resource with more demands than it can handle, consuming its available band-

width which results in server overload.

5) Phishing

This is a technique for extracting confidential information such as credit card numbers and username password combinations by masquerading as a legitimate organization [5].

6) Bombing and Spamming

Email blasting is characterized by the fact that an attacker sends huge amounts of email to a target address causing the victims' email account or mail servers to crash [5].

7) Jacking

Web jacking gets its name from hijacking. Here, the hacker is controlling the web site in a fraudulent manner [5]. He or she may change the original web site content or even redirect the user to another similarly-looking fake page that he controls.

8) Cyber Stalking

Cyber stalking is a new form of cybercrime in our society when someone is stalked or stalked online [5]:

a) Stalking the Internet,

b) Computer chase.

9) Data Diddling

Data Diddling is unauthorized alteration of data before or during entry into a computer system, and then altered again after processing has finished [5].

10) Theft and Credit Card Fraud

Identity theft occurs when someone steals your identity and pretends to be you to access resources such as credit cards, bank accounts and other benefits in your name [5].

11) Slicing Attack

Salami slicing attack or salami scam is a technique by which cybercriminals steal money or resources a little bit at a time so that there is no noticeable difference in the overall size.

12) Software Piracy

Internet piracy is an integral part of our lives which knowingly or unwittingly contribute to Cybercrime includes [5]:

- Illegal access
- The illegal interception system
- Interference data
- Interference with misuse of fraudulent devices.

3.2. Cyber Security Techniques

We introduce here some of Cyber Security Techniques as explained in **Figure 2**.

- **Access Control and Password Security**

The concept of user name and password has been fundamental way of protecting our information. This could be one of the first measures in terms of cyber security [1].

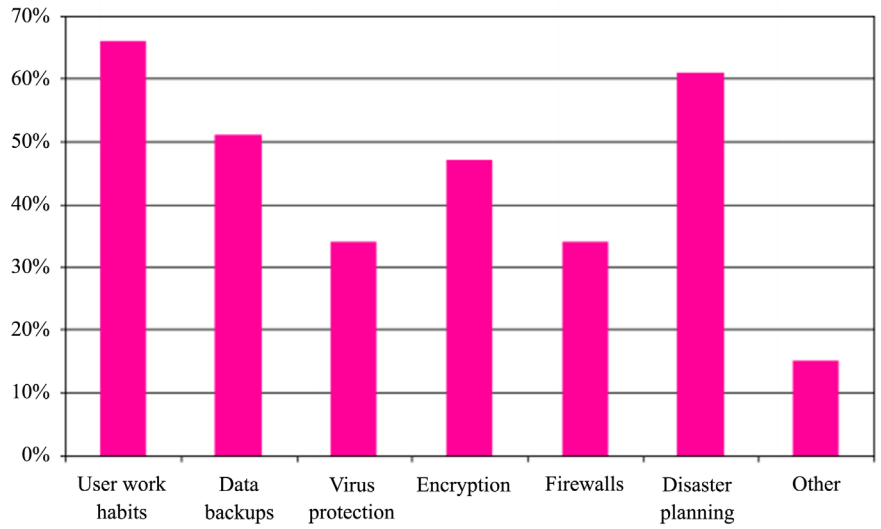

Figure 2. Techniques in cyber security.

- **Data Authentication**

The documents we receive must always be authenticated before downloading, and this must be verified if they originated from a reliable and a relative source and have been modified [1]. These documents are usually authenticated by the in-device anti-virus software. Hence good anti-virus software is also essential to protect the devices from viruses.

- **Malware Scanners**

This is the program that usually scans all the files and documents in the system for malicious code or malicious viruses [1]. Viruses, worms, and Trojan horses are examples of malicious that are often grouped together and referred to as malware.

- **Firewalls**

A firewall is a program piece of hardware that helps block hackers, viruses, and worms that try to access your computer over the Internet [1]. All messages entering or leaving the internet pass through the existing firewall, which checks every message and blocks messages that do not meet the specified security criteria. Hence firewalls play an important role in detecting the malware.

- **Antivirus Software**

Antivirus software is a computer program that detects, prevents, and takes measures to deactivate or remove malicious software, such as viruses and worms [1]. Most antivirus programs include an automatic update feature that enables the program to download new virus definition files so that it can scan for new viruses as soon as they are discovered. Antivirus program is a must and basic necessity for every system.

3.3. Cyber Ethics

Cyber ethics is nothing but a symbol of the internet. When we practice these internet ethics, there are good opportunities to use the internet in a safe and secure

manner [1] [2]. Here are just a few of them:

- Use the Internet to communicate and interact with others. Email and instant messaging make it easy to stay in touch with friends and family, communicate with co-workers, and share ideas and information with people across town or halfway around the world.
- Don't be an Internet bully. Do not call or lie to people, send those embarrassing pictures or do anything else to try to hurt them.
- Internet is the largest library in the world that contains information on any topic in any subject area, so using this information in a correct and legal manner is always necessary.
- Do not handle other people's accounts using their passwords.
- Never try to forward any type of malware to other's systems and make them corrupt.
- Never share your private information with anyone as there is a good chance it will be misused by others and in the end you may end up in trouble.
- When you are online, never pretend in front of the other person, and never try to create fake accounts on another person as this will lead to you and other person in trouble.
- Always adhere to copyrighted information and do not download games or videos unless permitted.

The above are some of cyber ethics that one must follow while using the internet. We always think that the proper rules from the very early stages are the same as we apply here in cyberspace.

3.4. Cyber Security Risks While Working Remotely

Before going into the tips, let us take a quick look at some of the most potential threats that you may face while working remotely [4]:

- There is no physical security.
- Communication gap.
- Concurrent VPN connections not supported.
- Lack of appropriate access, authorization, and authentication policies for implementation.
- Poor data backup implementation.
- Disk encryption for all endpoints.
- Wi-Fi connections are not secure.
- Easy logins and passwords.

3.5. The Best Practices to Overcome Cyber Security Risks?

To avoid being a victim of a cyber-attack, here are some best practices you must implement as illustrated in **Figure 3** [4].

1) Set up Firewalls

To prevent threats from entering your system, firewalls create a barrier between the internet and your computer [4]. It closes the ports of communication,

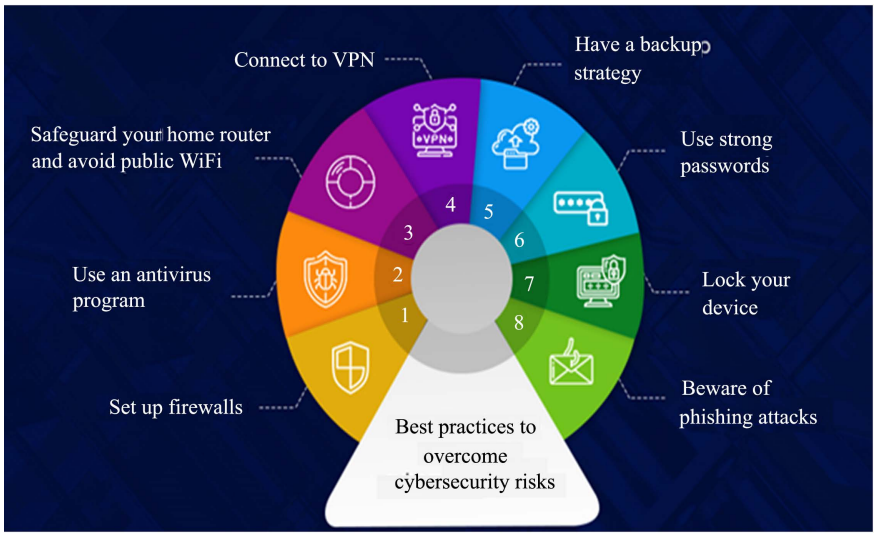

Figure 3. The best practices to overcome cyber security risks.

thus helping malware from getting in. While your computer already has a built-in firewall, it is important to verify that it is enabled.

2) Use an Antivirus Program

While a firewall can help, threats can still arrive. The next line of defense is to install a good antivirus program into your system to block and detect maliciously.

3) Safeguard Your Router and Avoid Public WiFi Networks

When was the last time you changed the WiFi password at home? (Or worse, is it password protected?) [4]. Changing your router password is one of the first steps you can take toward security. Be certain that:

- Encryption is set to WPA2 or WPA3
- Inbound & outbound traffic is constrained
- WPS is turned off

Make sure you not use public WiFi as it is mostly insecure and using it will result in being the victim of a man in the middle attack.

4) Connect to a Virtual Private Network (VPN)

Creating a secure tunnel between your computer and the ultimate destination on the internet, VPN allows you to send confidential information without any worries since it encrypts the entire internet connection [4]. By connecting to a VPN, you can connect to the internet easily without worrying about being eavesdropped on your sensitive information. VPN theory and practice in book (Zeeshan Ashraf, VPN in Theory and Practice Book, March 2018).

5) Have a Backup Strategy

Data loss is like doing tax: nobody likes it, but it's unavoidable. Data may be lost due to physical hardware damage, human error, cyber-attacks, or ransomware. Obviously, these reasons are enough to back up your data before you lose it forever. Although hardware backups are still popular, cloud backup is one of the most convenient ways to protect your data.

6) Use Strong Passwords

Having a strong password is the first line of defense [4]. Your password should be a perfect combination of upper and lower case letters, numbers, and special characters. It is good to make use of password managers like KeePass to help create, protect, and track strong passwords for your online accounts.

7) Lock Your Device

If you thought your laptops should be locked at work. It is absolutely essential that you lock your device if you live with people with whom you can't share business information [4].

8) Beware of Phishing Attacks

Phishing attacks were on the increase [4]. According to Barracuda Network researchers, a total of 9116 phishing attacks related to the epidemic have been directed. So, the next time you come across a link containing positive information about an epidemic treatment, beware! It most probably is a hacker.

4. Problem That Faces Sensitive Information Security in Cyber Physical System

Through our searching in cyber security threats, we found that there is a big problem that faces sensitive information security in cyber physical system even with using cryptographic techniques. Currently, there are problems with traditional encryption methods, such as [10]:

- Low speed for obtaining information;
- Low recognition rate;
- Low utilization rate of efficient information resources, and;
- Long delay in querying information.

4.1. Proposed Algorithm for Sensitive Information Security in Cyber Physical System

New developments in smart electronic cyber-physical systems can be demonstrated to include smart cities, the Internet of Things (IoT), and often anything smart. To improve the security of sensitive personal information (SPI) in cyber-physical systems, there are some new insights into SPI coding have been introduced. To address previous issues introduced in Section 4, we choose a proposed powerful new encryption algorithm for incremental SPI security as in [10]. First, the proposed method analyzes the user's information resources and determines which valid data will be encrypted. Next, it uses adaptive acquisition methods to gather information, and uses proposed cryptographic method to complete the secure encryption of SPI based on the acquisition results. Experimental analysis of the proposed algorithm clearly shows that the algorithm effectively improves the speed of obtaining information as well as the effective information recognition rate, thus enhancing the security of SPI. The encryption model, in turn, can provide a strong assurance of the security user information. The proposed new encryption algorithm looks to solve the following shortcomings in the existing encryption algorithms:

- Low speed data acquisition speed.
- The data recognition rate is low.
- Effective use of resources.
- Delays in data inquiries by traditional methods.

The proposed algorithm analyzes the user's data resources and encrypts the data according to the results of the analysis that measure the type of data involved. This effectively solves the problem of data query delays caused by traditional methods of encrypting large amounts of data by encrypting data that only needs to be enhanced security and privacy. To solve the problem of low data recognition rate and efficient use of resources, a quantitative interference method (described later) is used to determine the location of specified data after data encoding. Experimental results show that the proposed algorithm effectively solves the shortcomings of traditional methods, and can protect a users' privacy and information security. Traditional methods require a lot of manual intervention when encrypting information and the degree of automation is low. In addition to analyzing users' private data resources, this proposed algorithm uses adaptive data collection method to collect SPI, which can improve the degree of information encryption automation. This algorithm designs a new robust SPI encryption algorithm to mitigate such problems. The method first analyzes public data resources, private data resources, and mixed data resources in user data. From this analysis, it is concluded what resources should be encrypted and what data can be shared openly and unencrypted. The basic concept here is that not all data fall within the context of SPI, thus there is no need to waste computational resources to encrypt/decrypt them. Data analysis helps create a subset of user data targeted for sharing and the encryption method. User data resources are collected using an adaptive data collection method. Finally, the data encryption method based on interference quantization is used to complete the analysis on the secure encryption method for SPI. Flowchart in **Figure 4**.

4.2. Experimental Results and Analysis

4.2.1. Experimental Setup

Specific data provided by Google Dataset Search as source of experimental data [11]. Google Dataset Search can be thought of as a one-stop shop for dataset, which contains massive data of various sizes and types from sources such as NASA and ProPublica. The data source is comprehensive, so the dataset has a strong applicable value. With MATLAB 8.0, an experimental platform for large-scale data resources was built for interference estimation, and use for data manipulation. With the time of data acquisition, the rate of identification of information resource, the delay in querying of the information and the efficient use of resources as experimental indicators, the proposed method was compared with those peers from [12] [13] [14] [15] to verify the effectiveness of the proposed method. All methods from [12] [13] [14] [15] have been restarted and compared to the proposed method. All models were implemented in Matlab

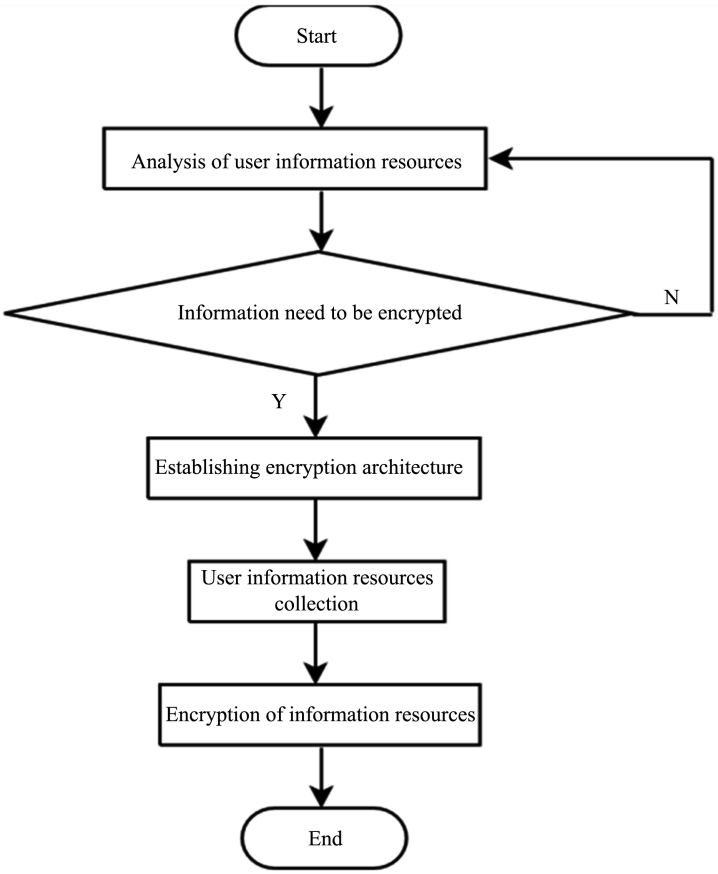

Figure 4. Secure encryption algorithm flow chart.

R2017b software environment and underwent processing and analysis as shown below.

4.2.2. Analysis the Experimental Results

Figure 5 shows a comparison of the data acquisition speeds of the proposed method with the peer methods in [12] [13] [14] [15]. In cases with the same amount of data, it was observed that a shorter acquisition time was associated with a higher efficiency of data acquisition. Therefore, they used the data collection time to check the collection efficiency. The specific results are shown in **Figure 5**. One of the elements worth noting here is that with an increase in information resources, most other methods show a linear increase in aggregating time, while the proposed method shows a more stable relationship that remains constant throughout the period of information increase.

The analysis of **Figure 5** shows that the time of data collection for the five methods varies. The method acquisition time in [12] ranges from1.4 s seconds and 4.2 seconds, and the acquisition time of the method given in [13] ranges from 2.1 seconds to 6.7 seconds. The time to obtain the method given in [14] ranges from 1.2 seconds and 10.8 seconds, and the time to collect private information is relatively long. The knock acquisition time [15] is between 4.5 seconds and 10.8 seconds.

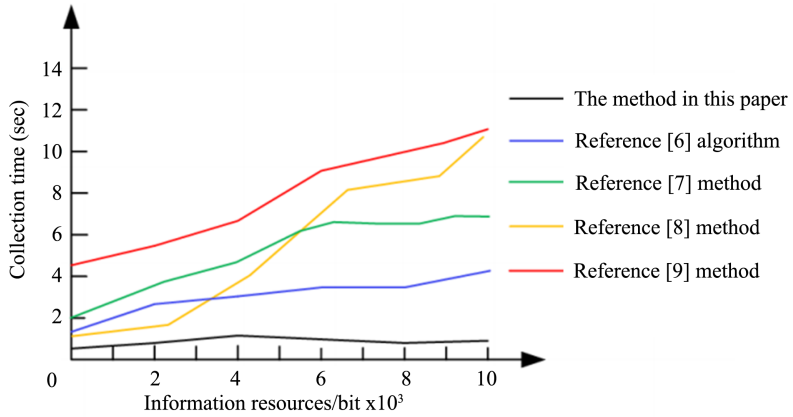

Figure 5. SPI collection time.

They attribute these valid data to the algorithm using the adaptive data collection method, which enables unity of decision during the execution of the data collection task, which saves a lot of time and meets the requirements of the task. To verify the accuracy of the data recognition methods, they again used algorithms from [12] [13] [14] [15] for comparison with the proposed algorithm under different data resource scenarios. The results are explained in **Figure 6**. The analysis of **Figure 6** shows that, when the resource quantity is 1×10^3 bit, the data recognition rates for the methods [12] [13] [14] [15] are 69%, 78%, 37%, and 36%, respectively. The data recognition rate for the proposed algorithm is 92%. When the resource amount is 6×10^3 bit, the data recognition rates for methods from [12] [13] [14] [15] are 59%, 80%, 62%, and 64%, respectively. Relatively speaking, the data recognition rate of the proposed algorithm is just over 90%.

It should be noted that this proposed algorithm uses mixed data resources, which means combining public data resources and private data resources [10]. User private data resources are linked with public data sources to create mixed user data resources. Specifically, the account includes personal account login, password, user ID card information, personal credit information, mailbox address and other information in public information. Private data resources belong to the privacy information of individual users, and cannot be obtained and used by persons other than public administration departments. Therefore, this algorithm mainly encrypts private data resources, and in order to protect user security, it is necessary to encrypt and protect sensitive personal information (SPI). Adaptive data collection method is used to collect the SPI. After instructions are sent to define the data collection tasks, the appropriate data collection tasks and decision-making unit are identified to meet the task needs. At the same time, privacy information is collected by the data processing unit to integrate resources [10].

By observing the overall graph in **Figure 6**, the data recognition rate of the algorithm is always best, indicating that the proposed algorithm has a high data recognition rate and good recognition performance [16]. They attribute this to

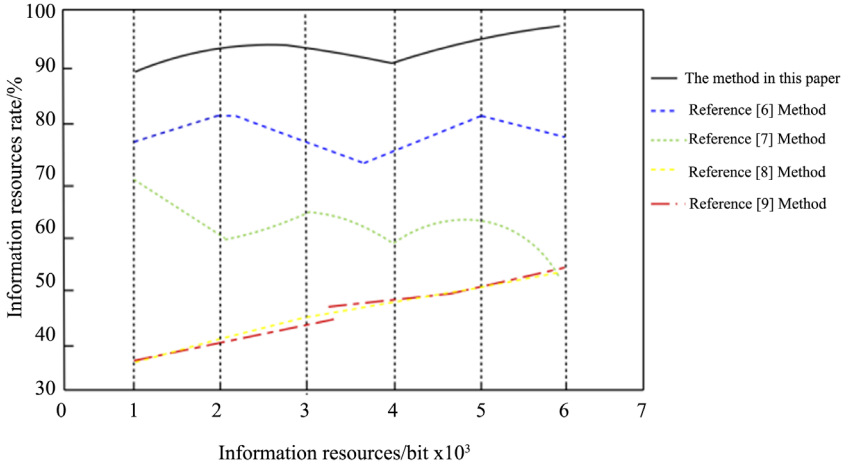

Figure 6. Recognition rate of information resources.

the fact that traditional information encryption needs to solve complex, non-convex optimization problems. However, the proposed method simplifies the problem in a way, which is known as interference encryption. To make the description more relevant, some auxiliary variables have been introduced, which reduce the influence of interference elements and improve the effective data recognition rate. One of the unexplained behaviors that should be noted is the decrease in the rate where the amount of the information source quantity is 4×10^3 bit; however, after this quantity, as anticipated, this is a little increase. This unfamiliar decrease may be attributed to some special manners of the algorithm at this amount of data. **Figure 7** explains a comparison of the delay caused by data resource queries in seconds for the proposed algorithm with the delays of [12] [13] [14] [15]. The analysis of **Figure 7** shows that the query delay of the five methods increases as the volume of data resources increases. When the private data used in the query is 6×10^3 bit, the SPI query delays of [12] [13] are 10.5 seconds, 8.5 seconds, 5.5 seconds, and 18 seconds, respectively. Likewise, the proposed algorithm creates a delay of only 3 seconds over 1 seconds. When the amount of private data used in the query reach 10×10^3 bit, the privacy data query is delayed from [12] [13] to 24.5 seconds, 16.5 seconds, 11.5 seconds, and 26 seconds, respectively. In comparison, the proposed algorithm creates a delay that is still around 1 second.

The user will not notice any change in delay even if the private data used in the query increases. This clearly indicates that the data resource query delay of the proposed algorithm is small, has better query performance, and is more feasible for large data storage applications. The performance of the proposed algorithm on a complete set of amounts of information resources is better than all comparable reference methods. **Table 1** shows a comparison of the information resource utilization rate (%) between the methods [12] [13] [14] [15] and the proposed algorithm.

Analysis of **Table 1** shows that the use of data resources for the four methods differs in the case of different quantities of private data [10]. When the private

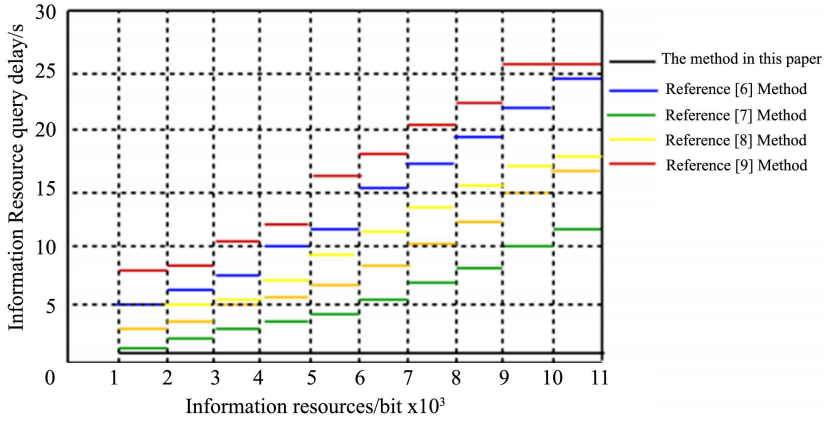

Figure 7. Privacy information query latency.

Table 1. Comparison of utilization rate of information resources of the proposed method with peers.

Privacy Information ($\times 10^3$ bit)	Methods				
	Reference [6]	Reference [7]	Reference [8]	Reference [9]	Methods (ours)
10	69	78	68	85	90
15	63	82	74	76	92
20	65	78	73	81	95
25	68	82	67	73	93
30	62	80	72	80	97

data are 10×10^3 bit, the resource utilization rates of [12] [13] are 69%, 78%, 68%, and 85%, respectively. In contrast, the resource utilization rate for the proposed algorithm is 90%. When the private data are 30×10^3 bit, the resource utilization rates of [12] [13] are 62%, 80%, and 72%, and 80%, respectively. Relatively speaking, the resource utilization rate for the proposed algorithm is 97%. It can be seen in **Table 1** that, regardless of the amount of private data, the resource utilization rate of the proposed algorithm exceeds 90%, and from this, it can be concluded that the resource utilization is strong.

Based on the above experimental results, chosen algorithm can effectively improve the private data collection time, increase the recognition rate of data resources, reduce the delay caused by private data queries, and increase the use of data resources. As a result, we can conclude that proposed encryption algorithm exceeds some of the current algorithms from [12] [13] in overall performance.

5. Conclusion and Future Work

The topic of the paper, cyber security, stands out merely by its title as an interesting and challenging area of research. The explanation for it is first and foremost that the area has not yet been sufficiently explored. Due to the intensive development of international relations in cyberspace, conditioned and supported

by the speed of the development of technologies and their implementation in the relations of states, organizations and individuals, this area will always be interesting and challenging. That conclusion arises from the constant change of attitudes and technology. A large number of international entities demonstrated their presence and willingness to act in cyberspace. Most authors predict an escalation of conflicts and intelligence activities in cyberspace. We could state that cyber-attacks are among the biggest threats to the international security. Unlike conventional conflicts, such attacks will become increasingly common, and they could, as a conventional attack, cause large-scale destruction, even with fatal consequences. It is therefore essential to establish an effective defense in which the key role is that of prevention, international cooperation and the adoption of the internationally recognized, legally binding norms. Due to the increase in cyber-terrorism and crime, we can conclude that cyber security has become one of the prerequisites of the democratic concept of life in the modern society, so it is necessary to organize systematic education and to strengthen operational military, intelligence, police and civil centers for the defense from cyber-attacks. There is no excellent solution for cybercrimes but we must do our best to minimize them in order to have a safe and secure future in cyber space. We introduced through our paper different challenges that face cyber security and different issues caused by cybercrime. We also introduced Proposed Algorithm to improve the security of sensitive personal information (SPI) in Cyber-physical systems and explained its novel results as illustrated in section 4. Future work, which is already in progress, is complete our study to the challenges that object cyber security, and how to overcome these challenges in order to exceed the maximum benefit from using cyber space technologies which will take title named (CybSec2) referring to complete searching in the same field of Cyber security because, as it is clear from the title we called this paper (SybSec1).

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Nikhita Reddy, G. and Ugander Reddy, G.J. (2014) A Study of Cyber Security Challenges and Its Emerging Trends on Latest Technologies. *International Journal of Engineering and Technology*, **4**.
https://www.researchgate.net/publication/260126665

[2] Duić, I., Cvrtila, V. and Ivanjko, T. (2017) International Cyber Security Challenges. 2017 40*th International Convention on Information and Communication Technology*, *Electronics and Microelectronics*, Opatija, 22-26 May 2017, 1309-1313.
https://doi.org/10.23919/MIPRO.2017.7973625

[3] Janczewski, L.J. and Colarik, A.M. (2008) Cyber Warfare and Cyber Terrorism. IGI Global, Hershey. https://doi.org/10.4018/978-1-59140-991-5

[4] Smriti Dewan (2020) Top 8 Tips to Overcome Cyber Security Risks.
https://www.grazitti.com/blog/top-8-tips-to-overcome-cybersecurity-risks-while-w

orking-remotely/

[5] Buch, R., Ganda, D., Kalola, P. and Borad, N. (2005) World of Cyber Security and Cybercrime. *Recent Trends in Programming Languages*, **4**, 18-23. http://www.stmjournals.com/

[6] Hewett, R., Rudrapattana, S. and Kijsanayoth, P. (2014) Cyber-Security Analysis of Smart SCADA Systems with Game Models. *Proceedings of the 9th Annual Cyber and Information Security Research Conference*, Oak Ridge, April 2014, 109-112. https://doi.org/10.1145/2602087.2602089

[7] Von Solms, R. and Van Niekerk, J. (2013) From Information Security to Cyber Security. *Computers & Security*, **38**, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

[8] Nigel, M. and Rice, J. (2011) Cybercrime: Understanding and Addressing the Concerns of Stakeholders. *Computers & Security*, **30**, 803-814. https://doi.org/10.1016/j.cose.2011.07.003

[9] Fischer, E.A. (2106) Cybersecurity Issues and Challenges: In Brief. https://fas.org/sgp/crs/misc/R43831.pdf

[10] Zhu, X.G., Srivastava, G. and Parizi, R.M. (2019) An Efficient Encryption Algorithm for the Security of Sensitive Private Information in Cyber-Physical Systems. *Electronics*, **8**, 1220. https://doi.org/10.3390/electronics8111220

[11] Google Search Central (2019) Dataset. https://developers.google.com/search/docs/data-types/dataset

[12] Zhang, C.L., Xiong, L. and Lu, L.C. (2018) Simulation of Double-Encrypted Reversible Concealment Algorithm for Real-time Network Information. *Computer Simulator*, **35**, 201-204+268. (In Chinese)

[13] Solomon, M. and Elias, E.P. (2018) Privacy Protection for Wireless Medical Sensor Data. *International Journal of Scientific Research in Science and Technology*, **4**, 1438-1442.

[14] Zhang, K., Douros, K., Li, H., Li, H. and Wei, Y. (2015) Systems and Methods for Pressure-Based Authentication of an Input on a Touch Screen. U.S. Patent No. 8988191.

[15] Qian, J.W., Qiu, F.D., Wu, F., Ruan, N., Chen, G.H. and Tang, S.J. (2016) Privacy-Preserving Selective Aggregation of Online User Behavior Data. *IEEE Transactions on Computers*, **66**, 326-338. https://doi.org/10.1109/TC.2016.2595562

[16] Sakhnini, J., Karimipour, H., Dehghantanha, A., Parizi, R.M. and Srivastava, G. (2019) Security Aspects of Internet of Things Aided Smart Grids: A Bibliometric Survey. *Internet Things*, Article ID: 100111. https://doi.org/10.1016/j.iot.2019.100111