Impact of Cyber Security Threats on Business and Government

PRABHDEEP SINGH
Assistant Professor, School of Computer Applications, BBD University, Lucknow, UP, India

Abstract- People and organizations are now more vulnerable to external attacks due to increased Internet use. In fact, most of the information systems, spyware, viruses, social engineering etc. It is affected by cybercrime in the form of various forms of malicious attack, such as The need for a more intuitive and automated system-level approach. It is the starting point of this study, which aims to determine the general characteristics of the security of an information system. In this article, we take our EAS-SGR framework designed to address security issues in IT governance systems and apply it to practice in cyberspace, with a focus on cybercrime. Our mission is to help governments, businesses and others reduce their vulnerabilities to acceptable levels by implementing a cybersecurity action plan.

Indexed Terms- Knowledge safety, Cybernetics safety, Hedirectory

I. INTRODUCTION

The terms "cybersecurity" and "cybersecurity" are similar but not completely interchangeable. Information security, as commonly understood, refers to the ability of an organization to secure the flow of information across its many departments, while cybersecurity refers to the ability to protect a user's assets and the environment in which they work to protect them from outside intruders. . one]. Cybersecurity has become a global concern lately and all countries have started creating programs about their involvement in cyber issues. At the same time, information security goes to great lengths to implement overall security goals . These goals include maintaining availability, integrity and confidentiality while ensuring accountability and auditability. While the definitions are somewhat comparable, the scope of each is different and increasingly broader than the others [2].

The structure of our contribution will be as follows: In the first section, we provide an overview of the current state of technology, focusing on the impact of cybersecurity on governments and businesses [3]. Next, we will discuss the huge financial damage caused by cybersecurity breaches . In the next section, we will provide a summary of some of the countermeasures used in the cybersecurity industry. In the second part of our talk, we will look at the key differences between information security governance and cybersecurity [4]. Next, we will review the new EAS-SGR-based framework and show how it will help us develop a cybersecurity action plan [5].

- SITUATIONFROMHEART

Information about the security of computer networks around the world

According to the majority of published articles, the importance of cyber security has increased significantly in recent years [6]. We are aware that many countries have adopted a system of security policies, tools and precautions to best prepare for the worst possible situation in cyberspace [7]. Cyberspace is an integral part of our daily lives; It is a high-speed network of wireless signals and local area networks installed in public facilities such as schools, hospitals, hotels, and government offices [8,9] The governments of some countries have made statements showing their awareness on this issue. According to President Obama , "the cyber threat is one of the most serious national security and economic problems we face as a nation" and "America's economic prosperity in the 21st century will depend on cybersecurity[10]".

The main goal of each country is to reduce the damage caused by cyber attacks and to make our systems more resilient to the impact of cyber attacks and events. Even high-level government officials can be affected by these problems [11]. For example, during the G20 summit, several diplomats accidentally infected their computers with malware when they clicked on a virus search email containing pictures of Carla Bruni-Sarkozy, who had previously served as the First Lady of France . [12].

We continue to observe that some officials still have insufficient knowledge of cybersecurity [13]. The main purpose of this document is to provide users with more information about the current state of information security in cyberspace.

- cyberneticsSafetyTo follow(Casualties)

"We must take steps to better defend ourselves against this threat," said Leon Panetta, who serves as the US Secretary of Defense [14]. Hacking and identity theft are only symptoms of a much larger problem that has the potential to escalate into a major attack on the United States. The American public should realize this [15].

Cyberattacks have been likened to storms in that they can destroy a city's critical infrastructure and bring an entire country to its knees. The weight of the losses is great because they came in the name of the nation. Additionally, Catherine Lotrionte of Georgetown University estimates that the annual transnational losses from intellectual property theft are approximately $300 billion [16].

Considering that one-third of the world's population is highly interconnected through various platforms, the impact of this issue on our nation will be enormous [17]. The lives of a significant number of people worldwide living in rural areas have the potential to be greatly improved by cyberspace [18]. People who are currently underrepresented online may be part of the next generation of Internet users.

The Internet itself is neutral; however, what we do while connected may not be neutral and may be the source of cyber attacks and other negative effects of using the service [19].

There is a significant amount of sensitive information stolen from businesses and governments around the world; these thefts are committed by organized networks and also by other nations [20].

Key questions for the future of cyberspace are, first, whether we need to create an approach that ensures the security and reliability of the Internet for our countries, and second, how we can ensure online security for our employees and their activities. without compromising openness, one of the most important advantages of the internet [22]. These are the two questions considered most important for the future path of cyberspace.

Informative context: IT security preventive measures FORWonderfulAreafromcountriesWITHstartedinvestmentInsidecyberneticsprecisionEastconsideredaspect DangerForherInformation systems and networks [23]. In this context, in 2011, the United States appointed a cyberspace coordinator named Harold Schmidt.

The field of cyber security covers a wide range of information and consists of a wide variety of disciplines [24]. Cyber security competitions are currently held all over the world and one of them is known as Cyber Security Challenge UK. Participants do not need to have any technical knowledge to join the company; However, common sense, logic, and the ability to identify and understand risk are essential assets. The primary purpose of these challenges is to test a wide variety of skills, but they all often share the same general themes, requiring participants to have an inquisitive nature, the ability to "think the unthinkable," and the ability to follow through in general. aim. , request. Aim at all costs [25].

Due to the sensitive information currently stored on our computers and servers, numerous standards have been established to help users and IT professionals protect the important information they hold [26]. These standards were developed in response to sensitive information currently stored on our computers and servers.

Many studies have been done in different parts of the world, and each has followed in the footsteps of the governments of the world's most powerful nations. Today, the vast majority of people are aware of this, thanks to research guided by the hierarchical models of the network, its applications and potential risks [27].

Researchers look at potential cybersecurity vulnerabilities from different angles. The Royal Institute of Technology (KTH) is hosting an ongoing research project that has resulted in the development of a cybersecurity tool [28]. CySeMoL is an acronym that stands for Cyber Security Modeling Language . It is both a modeling language and a software application that can be used for cyber security analysis in businesses. Users will be able to model their architecture using CySeMoL [29], which is the main focus of the program . Users can also predict the probability that certain cyberattacks will be effective. For calculations to be enforceable, customers only need to describe their system architecture (e.g., services, operating systems, networks, and users) and specify their characteristics (e.g., whether encryption is used and software is updated accordingly).) [31]. It has 102 features and 32 feature links in addition to its 22 features. In fact, it allows performing information security studies of enterprise architectures without requiring significant prior information security knowledge from the modeler. However, the model is still in the prototype stage and researchers are still working hard to expand its functionality to include time estimates for various attacks, web application attacks, and network vulnerability analysis. Further research has been done to develop a methodology that provides a method to automatically verify the correctness of cybersecurity applications using a formal, model-based hierarchical analysis of the network, its applications, and potential attacks [33]. This method represents a method for automatically verifying the accuracy of cybersecurity applications using a formal analysis based on the hierarchical models of the network, its applications, and potential attacks.

None of these studies use proven frameworks or techniques or build a hybrid model with multi-agent systems to add some intelligence to the processes under consideration. None of this happens. Therefore, in our cybersecurity strategy, we aim to create a robust complex that helps organizations, governments and institutions protect the critical information systems they manage [34].

- INFORMATION SECURITY AND CYBER GOVERNANCESAFETY

Since cybersecurity is such a broad field of study, we found it necessary to compile a list of some key concepts to gain a deeper understanding of the subject. To talk about the connection between ISG and cybersecurity, we need to create the concept of governance. Governance is the process of maintaining an effective institutional structure and the definition of the word can be found here [35]. Some important concepts related to governance are:

- basic idea
- the goal of the project
- transparency
- equity capital
- Responsibility
- company responsibility

These recommendations must be respected and followed, as every organization needs a clear vision of each of the tasks its employees must perform [36]. Only then can a company hope to achieve its business goals. Instead, the company's work team should communicate openly with each other and take responsibility for the consequences of their actions.

- Information Safety

Information security is considered the most valuable asset due to its well-known qualities such as Confidentiality, Integrity and Availability (CIA) [37]. In today's world, these criteria are not sufficient to address the nonsensical vulnerability circulating on the internet in terms of cybersecurity; however, the CIA's triangle model is no longer an acceptable response to the ever-changing environment of the IT industry." Therefore, we need to add new parameters such as accountability and auditing, and when this is done, CIAAA [38] Here is the definition of what add-ons:

- The condition for liability is that all activities performed by a company can be specifically attributed to that company. Indeed, any action or inaction of an employee can be linked to it.
- Auditing: Auditing security-related events is an important part of identifying and recovering from vulnerabilities and attacks.

Information Safety Governance (ISG)

ISG stands for Information Security and Corporate Governance and is a term used to describe the intersection of the two [39]. We are in a better position to deal with potential threats as we add accountability procedures and controls to the CIA's capabilities . Mark Brown, director of information security and risk assessment at Ernest and Young, was commissioned in 2013 to conduct an assessment of the company's use of information technology [40]. This review was conducted under the direction of Ernest and Young. The result of the investigation is as follows:

- 85% of respondents believe information security does not meet their business needs
- 88% of respondents saw an increase in the number of external threats.
- 57% of respondents say the number of insider threats is increasing
- 61% of respondents cite lack of funds as the main obstacle.
- 57% of organizations think their information security resources lack the necessary skills.
- 62% of organizations do not link information security to corporate architecture or business processes.
- 38% do not match the organization's risk appetite

Yet all cybersecurity researchers and professionals are doing everything they can to prevent risks from slowing or even hindering the way organizations achieve their business goals. As a matter of fact, this situation is still considered as the biggest obstacle in front of enterprises [41]. At the same time, the scope and scope of attacks continues to increase, penetrating even deeper into information systems in search of highly sensitive data.

Based on this analysis, we need to take a more thoughtful approach to managing IT risks and cyber security threats, as well as develop a new framework that helps IT administrators protect their systems and, more importantly, prevent them from being compromised. cybercriminal activities can be used. [42], which has recently become the center of the security industry.

- Cyber security data

While most people have only a limited understanding of the dangers posed by cybercriminals, the real impact of computer systems is enormous. Last year, 93% of large organizations and 87% of small businesses in the UK reported experiencing a cyberattack. These numbers should serve as a wake-up call as they are impressive and disturbing. The Secure Government Intranet Gateway (GSI) blocks more than 33,000 malicious emails from entering the secure government network each month. They are likely to contain advanced malware or links to websites that contain it. Every month, more and more spam and malicious emails, especially less advanced ones, are successfully avoided. With the costs of a cybersecurity breach expected to range from £450,000 to £850,000 for large UK companies and between £35,000 and £65,000 for smaller companies, we must look for new ways to defend business and make the world more resilient to cyberattacks and cybercrime [43] .

- NEW METHODOLOGY

In recent years, new computer security standards have been developed in response to the increasingly common practice of storing sensitive information on computers connected to the Internet. In fact, much work that was once done by hand is now done by a computer [44].

An architect or engineer usually sets a target security level before working on a system design [45]. This goal can be achieved by identifying and applying the operational criteria set out in each of the objectives and taking these actions with an appropriate "quality level".

Therefore, we have chosen to implement multi-agent systems that can provide the necessary intelligence to our framework to be able to adapt to various conditions, including cybersecurity [46].
multi agentsystem

Before proceeding to define a multi-agent system, you must first go through the process of defining an agent. An agent can be defined as a physical entity that can move autonomously, adapt to its environment, and communicate with other agents in these contexts [47].

organization defines the system's ability to perform tasks autonomously and respond to events. The organization of a system defines its ability to perform autonomous tasks and spontaneously respond to environmental events [48].

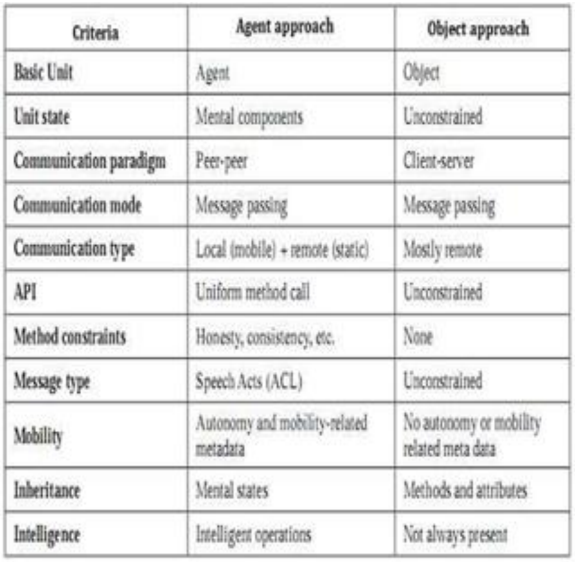
Our architecture must be able to both decide and react to situations . To meet this global criterion, the architecture must have the following properties[49]:

- Programmability: A viable control system cannot be set up for a single environment and cannot have a single job pre-programmed to the finest detail. You should be able to perform many tasks described at an abstract level. It shouldn't be difficult to combine functions depending on the job.
- change both the job at hand and his behavior according to the current goal and accepted practice scenario .
- Reactivity: the architecture must be able to accommodate events of limited duration consistent with the precise and effective achievement of its objectives (including its security). These constraints must be compatible with the architecture's ability to safely achieve its goals. Maintain Consistent Behavior: To maintain consistent behavior, the system's responses to cyberattacks must be driven by the goals of its activity.
- Reliability: The system must use redundant processing to be reliable. To achieve robustness it will be necessary to decentralize control to some degree .
- Extensibility: Adding additional features and developing new tasks should be a simple process. Learning skills are a very important consideration in this context; Architecture should be designed to enable learning capabilities.

As we observe here, an interesting relationship can be identified between the desirable features of our strategy to solve cybersecurity problems and the behavior of agent-based systems: Cybersecurity

- Agent-based techniques for creating software and algorithms have received a great deal of academic attention in recent years and are increasingly used in the design of complex systems. This interest can be attributed to the fact that multi-agent methods are easier to understand and apply than traditional approaches. This approach has led to an increase in the number of complex systems built using agent-based techniques.
- Agents rely on their personal experience and knowledge of the environment, as well as information obtained through interaction with the environment and other factors, when making decisions.
- It results from adopting a local perspective in decision making while maintaining independence from the centralized form of control .
- Due to the distributed nature of this approach, it also offers a degree of fault tolerance. This includes problems from the software/hardware system itself as well as from the wider environment.
- Self-organization and complex behaviors can be represented by multi-agent systems even if the individual strategies of all individuals in the system are fairly simple.
- Agents are free to exchange information in any agreed language within the system's communication protocol settings. Two examples of such languages are Knowledge Query Manipulation Language (KQML) and Agent Communication Language (ACL) developed by FIPA .

illustrates the reasons for our decision to use an agent-based framework [50]:



Criteria	Agent approach	Object approach
Basic Unit	Agent	Object
Unit state	Mental components	Unconstrained
Communication paradigm	Peer-peer	Client-server
Communication mode	Message passing	Message passing
Communication type	Local (mobile) + remote (static)	Mostly remote
API	Uniform method call	Unconstrained
Method constraints	Honesty, consistency, etc.	None
Message type	Speech Acts (ACL)	Unconstrained
Mobility	Autonomy and mobility-related metadata	No autonomy or mobility related meta data
Inheritance	Mental states	Methods and attributes
Intelligence	Intelligent operations	Not always present

FIGURE 1.agentfocus on the other side article Come closer

Our preference is for intelligent, autonomous, enterprise-grade, communicating multi-agent systems, as well as systems that mapping demonstrates and validates with these properties.

- To apply Forcy bernetics Safety make a plan

Companies make every effort to ensure the security of their information systems at the highest level and
The purpose of the framework is to define which aspects of safety expertise should be included and which can be outsourced. It will consider all aspects of hazards and threats to help organizations develop an information security strategy that limits risk.

In our most recent work, we looked at a framework made up of four different multi-agent systems. The following sections provide a brief overview of each of these multi-agent systems.

- Security Controllers MAS (Multi-Agent System): It consists of three agents in total. The first representative is the person responsible for compiling a list of rules and regulations that a company operating in a particular country must follow to avoid legal trouble. The second officer outlined the company's business objectives and emphasized the importance of security to ensure the company's assets are protected and its data remains confidential; this contributes to the success of the company in achieving its corporate goals. The third party is responsible for collecting the remaining threats, which could potentially be the source of an attack on the information system. This multi-agent system depends on a knowledge base to function properly.
- Definition of SMA controls: The first tool helps define the information system's security policy that needs to be modified according to business objectives and business drivers. This is necessary to ensure system security. Compliance with this policy at all times is essential to protect the organization . The second agent should accept the general catalog of controls and will include a list of preventive actions that should be taken to support the policy.
- MAS Risk Management – This multi-agent system manages all parts of the risk management process, including risk identification and assessment, risk processing, risk acceptance, risk reporting and review, and auditors. These components also include risk communication .
- MAS Metrics Management: This multi-agent is responsible for implementing security measures, executing an action plan, sharing results, and preparing reports. Also, report generation is the responsibility of this multi-agent system.

The highest level of our architecture is represented by the interface agent. According to the overall mission, you should establish a set of goals or missions (business objectives) for activities.

but we aim to change it to apply to cyber security. The procedures to follow to create a defensive barrier against cyber attacks and cybercrime in general are listed in Table I shown below.

TABLE 1 . ACTION MAKING A PLAN FOR CYBERSAFETY

Part of the multi-agent system	Definition
MAS safety controllers	Follow the rules and laws set for the Internet.
MAS safety controllers	Emphasize cybersecurity as a management priority by design
MAS safety controllers	Set up a monitor for attacks on your computer's security.
SAM definition checks	Create a privacy protocol for employees.
SAM definition checks	Address cybersecurity issues .
SAM definition checks	A cybersecurity policy that operates in an international context
SAM definition checks	Discuss various cybersecurity policies, opportunities and measures.
SAM risk management	Cyber incidents need to be prevented, then detected and then evaluated.
SAM risk management	Developing a cybersecurity and privacy-sensitive identity management vision and strategy,
SAM risk management	Face the situation and determine how to accept it.
Manage MAS metrics	Create a plan to respond to any cybersecurity incident.
Manage MAS metrics	Establish permanent benchmarks for performance evaluation.
Manage MAS	Reporting intruders and potential

metrics	cyber attacks to senior management is a strategic responsibility.
Manage MAS metrics	Cybersecurity check against current attacks

define roles and tasks and delegate certain tasks to each manager and supervisor. In fact, according to MAS's definition of control, we are required to appoint an information security policy officer who shares responsibility with others.

TABLE 2.TEAM _MEMBERS

Roles	Responsibility
Responsible for IT security assessment	Manages the cybersecurity assessment process, coordinates activities, and plans a report using feedback from all team members.
system administrator	Performs technical maintenance of the system.
technical evaluator	Understands the technical components of the system but was not involved in the creation of the system.
Owner of a systems company	is responsible for the operation of the system or the quality of the services provided. You know the general purpose of the system, but you do not know the details.
technical owner	Accept the leadership role and responsibility of the system.
General manager	responsibility rests with top management.
information security manager	Responsible for security policies and objectives.

The influence of cyberspace is almost everywhere and on everyone. Therefore, Annex II and the Information Security Governance Responsibility function require the assignment of roles and responsibilities to project owners within the organization as well as those responsible for risk management .

How agents work together and communicate with each other through their environments is shown in the figure below, Figure 2.

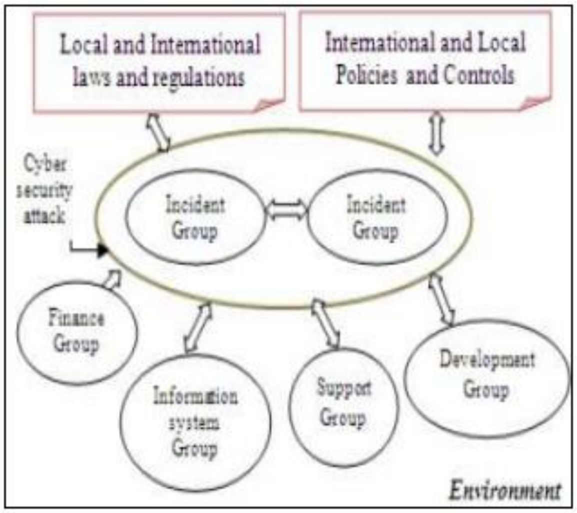


FIGURE 2Collaboration and knowledge sharing within MAS groups within an organization

highlights the importance of using multi-agent systems to create collaborative teamwork to successfully overcome the challenges of cybercrime . In fact, the work carried out by the team must conform and comply with the rules and regulations of the local and foreign communities .

CONCLUSION

In this article, we talk about a big problem that most of the world's nations are facing now and will continue to face in the years to come, and that problem is cybercrime. As part of our discussion, we examine the field of cybercrime and highlight the challenges of cybersecurity . Indeed, this obstacle seems difficult and almost impossible for most nations to overcome. Instead, researchers apply various countermeasures to prevent or reduce the negative effects of cyber attacks.

REFERENCES

[1] BrianPrince, Cybersecurity Reporthighlight progressTo come,E-week 2010

[2] Patrick Tibodeau , Cyberattacks Might Cripple the U.S., Legacy Defensebosswarns: “Computer World2014

[3] Giuseppe Macri , "SXSW spokesperson says government officials knowNOTHINGabout cyber security", HEDaily Call , 2014.

[4] 2013NSACapacityForHEBetterscientistInternet Safetypaper pictureWeb site,2012

[5] London Cyberspace Conference, Vice President Biden, “VicePresident Biden speaks at London conferencecyberspace

[6] Web siteFor"PriceForcyberneticsSafetyChallenge”, United Kingdom, 2013

[7] Holm, H. , Somestad , T.; Ekstedt , M.; Nordström , L.; " Cisemolo : aToolForcyberneticsSafetyanalyzesfromCompany" Rwantfromtechnology,percentageFromHE22InternationalconferenceANDexposureInsideelectricDiffusion, 2013, Stockholm

[8] von Solms R, van Niekerk J, From information security to cyberneticssecurity, informatics, etc.Safety(2013) aSuppress,

[9] hacker Iguer , Hicham Medrom and Fair Sayuti , "The Effects4th wave of information systems governance: IT risksArchitectural-SAE– According to the RMS value Insidemultiple agentsSystems", InternationaldailyfromcomputertheoryANDmechanical EngineeringFlight.6,NO.5,Pages.432-437,2014

[10] Gustavo Alberto de Oliveira Alves , Luiz Fernando Rust da CostacarmoANDmomChristinaribeirodutraby Almeida« Corporate Security Governance : A Practical Guide to Implementation and AuditinformationSafetydirectory(GSI) »HEFirstIEEE/IFIPInternationalGarageInsidebusiness orientedHETo manage,2006IMDB extension'06page 71-80

[11] Mark Brown, Director of Information Security and Risk Management ConsultingReally&young", *companySafetyArchitectural"*,computerweekly

[12] Gary Stoneburner "Basic technical models for knowledgeTechnological Security » NIST Special Publication 800-33, ComputersSafety

[13] galenascratch ,Irelandall winemiguelmarshes,LIKEFIG, "model-basedcyberneticsSafety",Acts of the Apostlesfromon the 14thYearlyIEEE International Conference and Engineering Workshopfromcomputer-basedsystems(ECBS'07),2007

[14] "Keeping the UK Safe in Cyberspace" National CybercrimeUnit(NCCU), June2014

[15] sagut ,a _,medromy ,H"SectionQualification:autonomousANDIntelligent mobile systems based on multi-agent systems, bookTitle: Multiple agentssystems - modelling,Check,Programming,simulationsANDApplications", INTECH,2011

[16] Sayouti , A., Qrichi Aniba , F., Medromi , H., Radoui , M. "Télé-Robotics over the Internet based on a multi-agent system", Proceedingsseventh international conference on distributed computingANDapplicationsForBusiness,mechanical EngineeringANDscience(DCABES), Dalian,China (yearbroadcasting:2008).

[17] Iron,I"multi-mediatedsystems,AloginFordistributedartificiallyIntelligence", Addison-Wesley,1999

[18] Navaneetha Krishnan Rajagopal , Mankeshva Saini , Rosario Huerta-Soto, Rosa Vílchez-Vásquez , JNVR Swarup Kumar, Shashi Kant Gupta, Sasikumar Perumal , "Human Resource Demand Configuration and Forecasting Model Based on Gray Wolf Optimization and Recurrent Neural Network", Computational Intelligence and Neuroscience, Vol. 2022, document ID 5613407, 11 pages, 2022. https://doi.org/10.1155/2022/5613407

[19] Navaneetha Krishnan Rajagopal , Naila Iqbal Qureshi, S Durga , Edwin Hernan Ramirez Asis , Rosario Mercedes Huerta Soto, Shashi Kant Gupta, S Deepak, "The Future of Entrepreneurial Culture: An Artificial Intelligence-Based Digital Framework for Organizing Decision Making of the company", Complexity, vol 2022 , document id 7796507, 14 pages, 2022. https://doi.org/10.1155/2022/7796507

[20] EshragRefaee , Sabana Parveen , Khan Mohamed Jarina Begum, Fatima Parveen , M.

Chithik Raja, Shashi Kant Gupta, Santhosh Krishnan, "Secure and Scalable IoT Health Data Transmission Based on Optimized Routing Protocols for Mobile Computing Applications," Communications Wireless and Mobile Computing, Vol. . 2022, document ID 5665408, 12 pages, 2022. https://doi.org/10.1155/2022/5665408

[21] Rajesh Kumar Kaushal , Rayat Bhardwaj , Naveen Kumar, Abeer A. Aljohani , Shashi Kant Gupta, Prabhdeep Singh, Nitin Purohit , "Using Mobile Computing to Provide an Intelligent and Secure Internet of Things (IoT) Framework for Medical Applications", Wireless Communications and Mobile Computing, vol. 2022, document ID 8741357, 13 pages, 2022. https://doi.org/10.1155/2022/8741357

[22] Bramah Hazela et al. 2022 ECS Trans. 107 2651 https://doi.org/10.1149/10701.2651ecst

[23] Ashish Kumar Pandey et al. 2022 ECS Trans.107 2681 https://doi.org/10.1149/10701.2681ecst

[24] GS Jayesh et al. 2022 ECS Trans.107 2715 https://doi.org/10.1149/10701.2715ecst

[25] Shashi Kant Gupta and others. 2022 ECS Trans. 107 2927 https://doi.org/10.1149/10701.2927ecst

[26] S Saxena , D Yagyasen , CN Saranya , RSK Boddu , AK Sharma and SK Gupta, "Hybrid Cloud Computing for Data Security System", 2021 International Conference on Advances in Electricity, Electronics, Communication, Computing and Automation (ICAECA), 2021, P 1-8, doi : 10.1109/ICAECA52838.2021.9675493.

[27] SK Gupta, B Pattnaik , V Agrawal , RSK Boddu , A Srivastava , and B Hazela , 'Malware Detection in the Internet of Things Using the Cascading Support Vector Machine Classifier', 2nd International Conference on Computer Science, Engineering and Applications 2022 (ICCSEA), 2022 , pp. 1-6, doi : 10.1109/ICCSEA54677.2022.9936404.

[28] Natarajan , R.; Lokesh , GH; Flamini , F.; Premkumar , A.; Venkatesan , United Kingdom; Gupta, a new framework for improving energy and security based on Medical Internet of Things 5.0 for SK Healthcare. *Infrastructure* 2023 , *8* , 22. https://doi.org/10.3390/infraestructuras8020022

[29] VS Kumar, A Alemran , DA Karras , S Kant Gupta, C Kumar Dixit & B Haralayya , "Natural Language Processing using Graphical Neural Network for Text Classification", International Conference on Knowledge Engineering and Information Systems Communication (ICKES), by 2022, Chickballapur , India, 2022, p. 1-5, doi :10.1109/ICKECS56523.202.10060655.

[30] M Sakthivel , S Kant Gupta, DA Karras , A Khang , C Kumar Dixit, and B Haralayya , "Solving Vehicle Routing Problem for Intelligent Systems Using Delaunay Triangulation", International Conference on Information Engineering and Communication Systems (ICKES) del 2022, Chickballapur , India, 2022, p. 1-5, doi : 10.1109/ICKECS56523.2022.10060807.

[31] S Tahilyani , S Saxena , DA Karras , S Kant Gupta, C Kumar Dixit & B Haralayya , "Using Autonomous Vehicle Deployment in Agriculture and Voronoi Divisions", International Conference on Information Engineering and Information Systems Communication (ICKES), 2022 , Chickballapur , India, 2022 , s. 1-5, doi :10.1109/ICKECS56523.202.10060773.

[32] Kumar, A Alemran , SK Gupta, B Hazela , CK Dixit & B Haralayya , SIFT function extraction to identify disaster-affected areas using machine learning techniques, 2022 International Conference on Information Engineering and Communication Systems (ICKES), Chickballapur , India, 2022, P 1 -5, doi : 10.1109/ICKECS56523.2022.10060037.

[33] VS Kumar, M Sakthivel , DA Karras , S Kant Gupta, SM Parambil Gangadharan and B. Haralayya , "Drone Surveillance in Flood-Affected Areas Using Firefly Algorithm", International Conference on Information Engineering and Communication Systems (ICKES) 2022, Chickballapur , India, 2022, p. 1-5, doi :10.1109/ICKECS56523.20202.10060857.

[34] equal Somani , Sunil Kumar Vohra , Subrata

Chowdhury , Shashi Kant Gupta. " Implementing a blockchain-based smart shopping system for automatic invoicing using smart shopping carts with cryptographic algorithms ." CRC Press, 2022. https://doi.org/10.1201/9781003269281-11.

[35] shivlal Mewada , Dhruva screenshot Chakravarthi , SJ Sultanuddin , Shashi Kant Gupta. " Design and implementation of an intelligent healthcare system using blockchain technology with a Blowfish encryption algorithm based on Dragonfly optimization ." CRC Press, 2022. https://doi.org/10.1201/9781003269281-10.

[36] Ahmed Muayad Younus , Mohanad SS Abumandil , Veer P Gangwar , Shashi Kant Gupta. " Artificial Intelligence Based Intelligent Education System with Self Adaptive Jumping Algorithm Developed for the Smart City ." CRC Press, 2022. https://doi.org/10.1201/9781003252542-14.

[37] Rosak-Szyrocka , J., Żywiołek , J. and Shahbaz , M. (editors). (2023). Quality Management, Value Creation and the Digital Economy (1st ed.). . _ https://doi.org/10.4324/9781003404682

[38] Dr Shashi Kant Gupta, Hayath TM., Lack of infrastructure for ICT-based education as an emerging problem in online education, TTICTE. July 2022; 1(3):19-24. Published online July 2022, doi.org/10.36647/TTAICTE/01.03.A004

[39] Hayath TM, Dr. Shashi Kant Gupta, Pedagogical principles in learning and their implications for improving student motivation, TTICTE. October 2022; 1(2):19-24. Published online July 2022, doi.org/10.36647/TTAICTE/01.04.A004

[40] Shayly Malik , Dr. Shashi Kant Gupta, "The Importance of Text Mining for Service Management", TTIDMKD. November 2022; 2(4):28-33. Published online November 2022 doi.org/10.36647/TTIDMKD/02.04.A006

[41] Dr Shashi Kant Gupta, Shaily Malik , "Application of Predictive Analytics to Agriculture", TTIDMKD. November 2022; 2(4):1-5. Published online November 2022 doi.org/10.36647/TTIDMKD/02.04.A001

[42] Dr Shashi Kant Gupta, Budi Artono , "Bioengineering in the development of artificial hips, knees and other joints. Ultrasound, MRI and other medical imaging techniques", TTIRAS. June 2022;2(2):10-15. Published online June 2022 doi.org/10.36647/TTIRAS/02.02.A002

[43] Dr Shashi Kant Gupta, Dr ASA Ferdous Alam , “E-commerce standardization concept and general process” TJAEE 2022 August; 1(3):1-8. Published online in August 2022

[44] Brian Prince, Cybersecurity Report Highlights Progress, Future, eWeek , 2010

[45] Patrick Tibodeau , Cyberattacks could paralyze the United States, Former defense chief warns , ComputerWorld , 2014

[46] Giuseppe Macri , "SXSW President Says Government Officials Know Nothing About Cybersecurity," The DailyCaller , 2014.

[47] Best Scientific Cybersecurity Report, official site, 2012.

[48] London Cyberspace Conference, Vice President Biden, “Vice President Biden speaking at the London Cyberspace Conference

[49] Cyber Security Challenge Awards Website, UK, 2013

[50] Holm, H. , Somestad , T.; Ekstedt , M.; Nordström , L.; " Cysemol : A Cybersecurity Analysis Tool for Business " R. Institute of Technology, Proc. Excerpt from the 22nd International Power Distribution Conference and Exhibition , 2013, Stockholm