IJAER/March-April-2022/Volume-11/Issue-2 ISSN: 2278-9677

International Journal of Arts & Education Research

LEGAL FRAMEWORK FOR CYBER SECURITY AND PRIVACY IN THE DIGITAL AGE

Siddharth Sagar,

Research Scholar, Department of Law,

Maharaj Vinayak Global University, Jaipur.

Dr. Anirudha Ram,

Supervisor, faculty of law

Maharaj Vinayak Global University, Jaipur

Abstract

The term "digital age" refers to a collection of various technological solutions such as "virtual environments," "digital services," "intelligent applications," "machine learning," and "knowledge-based systems," among others. These technological solutions are what determine the specific characteristics of the contemporary world, such as globalisation, e-communications, information sharing, and virtualization, among other things. However, there is a possibility that the technologies of the digital age would break some of the fundamental principles of information security and privacy. This might occur as a result of unrestricted access to information and personal data that is kept at various nodes of the global network. The purpose of this article is to identify certain unique aspects of the protection of information and personal data and to provide a synopsis of the most significant difficulties posed by the digital era to the user's security and privacy. The provisions of The Information Technology Act, 2000, which was enacted in the primary interest of facilitating e-commerce and Electronic Governance, gave only a very cursory treatment to the problem of protecting people's privacy in cyberspace. In the declaration of aims and reasons, it was said that there was a need to put in relevant revisions to support e-commerce. This necessity was mentioned. In addition, it said that there was an attempt to avoid misuse over transactions in electronic media and that civil and criminal responsibilities had been imposed for disobedience of the terms of the Information Technology Act. There were provisions for breaches of privacy and confidentiality included in Section 72.

Keywords: *Cyber, security, digital age*

Introduction

The rapid rate at which the laws of our economy and many of the processes that make up our society have been transformed as a result of the digitalization of virtually every aspect of our society. This revolution has been made possible by contemporary Information and Communication Technologies (ICT) as well as advancements in microelectronics, which, when combined with the networking of billions of individuals, has resulted in this transition. The process of digitalization and transformation is gaining further momentum through the networking of numerous physical objects that are becoming the Internet of Things (IoT) and what could be in the future the Internet of Everything, as objects are going to have an increasing amount of intelligence and people and objects will be constantly connected with one another. Everything is moving towards a more or less complete digital transformation. Because of these advancements, there is a significant opportunity to establish new applications, enterprises, and channels for the flow of wealth. However, the dangers that our digital systems face have also undergone significant shifts and have become more severe. Not only does this pose a threat to our information technology systems, but it also poses a threat to our physical world and the privacy of our personal information as more and more of our physical environment becomes digital and linked. Because our future industry, transportation systems, smart cities, power plants, energy networks, and other infrastructure will depend fully on safe and secure systems, cybersecurity will also become a key safety concern for our digital control systems in many facets of our daily lives. Safety-critical control systems, such as those used in industry 4.0, the automotive industry, the aviation industry, and the marine industry, are already demanding new approaches and tools for the creation of safe and secure systems, and they will even define new rules as a result. Cybersecurity is going to become a problem that is not only essential for ensuring the safety of our new digital vital systems, but it is also going to be a precondition for establishing confidence in our digital economy. Both of these things are going to be very important. It will be a significant aspect in determining the global competitiveness of goods, systems, and ubiquitous services because of its central role in ensuring the resilience of these things. The present COVID-19 issue has been accompanied by new patterns of cybercrime, the majority of which are the result of an increase in the intensity of teleworking and e-commerce. Cyberattacks that have taken place all over the world have demonstrated how fragile our society and economy have become, as well as the fact that even huge organisations and governments are having difficulty coping with cyberthreats. Because the effects of a cyberattack can potentially erode the faith that people have in digital systems, the running of both our economy and our society is becoming increasingly dependent on the state of cybersecurity. In addition, the digital infrastructure of Europe relies largely on systems that were established in Asia and the United States at the present time. However, neither users nor governmental authorities have complete control over the degree of security provided by these systems or the data protection procedures that are in place. There is a growing fear that Europe's digital sovereignty may be at risk, and there is also a growing concern that cybersecurity and privacy protection are developing too slowly to keep up with all of these difficulties.

Major challenges and needs

Cybersecurity is inextricably linked to demanding standards in an environment that is notoriously complicated. In spite of the fact that cybersecurity is a business that is expanding on a worldwide scale, Europe's cybersecurity sector is dominated by a small number of global firms and has a decentralised research and development environment. On the other hand, public investment, which includes research in cybersecurity, is quite low in comparison to the investments that are being made in other regions of the world, such as the United States or China. When we take into account the fact that cyber threats are global and cross-national, that new threats are constantly emerging, that threat patterns and associated technologies are evolving at a rapid rate, and that new application areas bring with them new vulnerabilities and additional attack surfaces, we have no choice but to acknowledge that Europe is in a precarious position when it comes to the fight against cyber threats. Cyberdefenders are in a constant race with cyberattackers to innovate new ways to carry out their responsibilities in light of the fact that cyberattacks are getting increasingly complex and making use of the most recent technology. Therefore, breakthrough technologies connected to cybersecurity, such as cryptography, artificial intelligence/machine learning/deep learning, and quantum technology, are essential, as are new methods for creating future systems with cybersecurity and privacy as design goals from the beginning. In this competition for innovative dominance, the function of R&D is of the utmost importance.

A comprehensive approach to ensure secure and safe systems

It is necessary to take a holistic approach to the problem of ensuring the safety and security of digital ecosystems. This approach must not only take into account advances in technology, but also organisational and legal considerations:

- An ecosystem for collaborative research and development that spans the entirety of the supply chain;
- Widespread use of tested processes and tools for the design and development of safety and security systems, as well as their operation;
- Legal frameworks, national and international policies
- Procedures for obtaining certification as well as standards
- Raising awareness and bolstering the capabilities of a diverse range of users (industrial, private, governmental, etc.)
- Making it easier for individuals to take charge of their own cyber security

In this regard, research and development creates the groundwork for advancement in the following important areas, each of which complements the other to accomplish safety and security in the digital age (refer to Fig.1 below):

- We need extensive threat catalogues for our digital systems, which are continuously updated by scalable tools and methodologies by industry professionals (ranging from system developers to security researchers), or even Artificial Intelligence (AI)-based search tools that continuously analyse a variety of information sources that are available on a global scale.
- The usage of encryption ought to be expanded to include a far larger range of scenarios in order to guarantee the genuineness, integrity, and secrecy of data in order to facilitate the highly secure transfer and archiving of information. Quantum Key Distribution (QKD) and other post-quantum encryption technologies are the primary forces behind the development of this sector.
- Safety, security, and privacy-by-design methods and model-based low-code system development techniques will allow a new generation of systems and provide the basis for successful testing and system certification, including cyber security and privacy by design of AI systems. These methodologies will also enable model-based low-code system development approaches.
- It is required to develop new, effective tools that are based on AI for real-time monitoring of digital as well as analogue systems. This is necessary in order to identify potential dangers as early as possible and to keep operational systems safe and secure.
- In order to be able to effectively fight against cybercrime, espionage, and terrorism in our future digital universe, law enforcement agencies (LEAs) and other governmental stakeholders will require new competencies as well as instruments.

Finally, advanced training services and platforms for various industries, service operators, critical infrastructure operators, citizens, and government stakeholders are essential support measures that will strengthen the capacities required to build, operate, and use our future digital systems in a highly secure manner. These support measures are essential because they will strengthen the capacities required to build, operate, and use our future digital systems in a highly secure way.

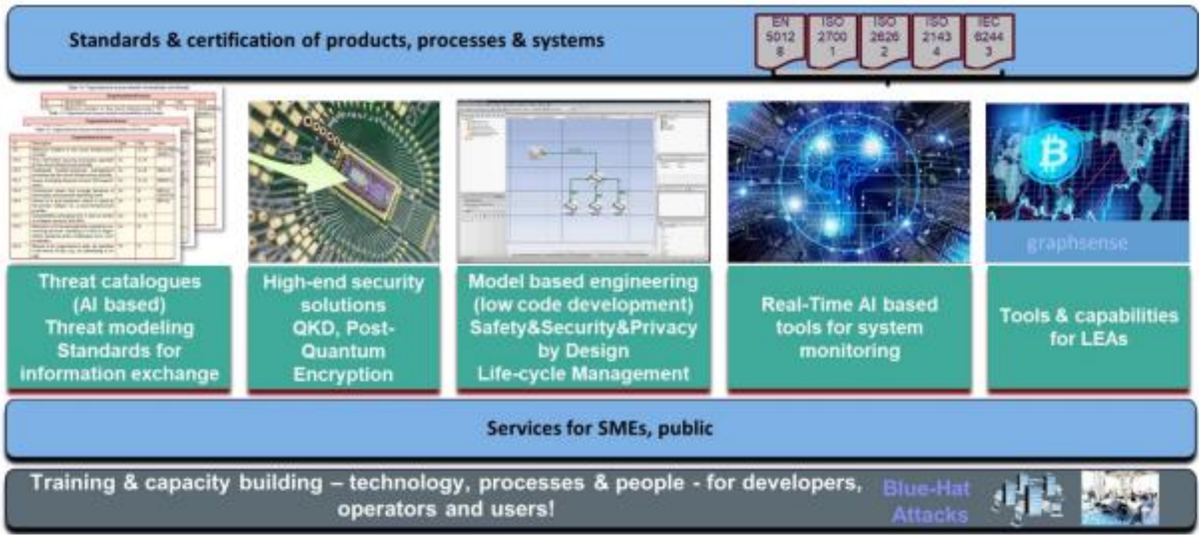
Standards & certification of products, processes & systems
EN 5012 8
ISO 2700 1
ISO 2626 2
ISO 2143 4
IEC 6244 3
Threat catalogues (AI based) Threat modeling Standards for information exchange
High-end security solutions QKD, Post-Quantum Encryption
Model based engineering (low code development) Safety&Security&Privacy by Design Life-cycle Management
Real-Time AI based tools for system monitoring
graphsense
Tools & capabilities for LEAs
Services for SMEs, public
Training & capacity building – technology, processes & people - for developers, operators and users!
Blue-Hat Attacks

Fig.1: An all-encompassing strategy for ensuring the safety and security of systems

2. Digital India programmer

On July 1, 2015, Prime Minister Narendra Modi announced the Digital India project of the Government of India programme with the intention of moving away from paper-based work in the nation and towards electronic-based work instead. This was done with the goal of eliminating paper-based work in the country. According to the official website of the government of India, it is a flagship plan with the goal of transforming India into a digitally enabled society and knowledge economy. This goal is stated on the website. The primary goal of this initiative is to guarantee that individuals will have access to the government's services in an electronic format, which will be accomplished through increasing the availability of high-speed internet and enhancing online infrastructure. The availability of a facility with a high-speed internet connection, a mobile phone and a bank account, an internet identity, access to a shared service centre, and a safe and secure cyberspace will all be part of the digital infrastructure. The Department of Electronics and Information Technology within the Indian government is responsible for the project's general coordination. Digital India encompasses a number of different government ministries and departments. Every rural community will have access to high-speed internet and broadband connections capable of supporting high speeds. It is planned to improve the technological infrastructure in order to provide digital identities to users of mobile phones and financial services accessible via mobile devices. Within the communities itself, there would be convenient entry points to shared service centres. The provision of opportunities for universal digital literacy is the goal of this endeavour. On cloud platforms, digital versions of all government and public documents will be made available to the public. In conclusion, the objective is to make the nation's cyberspace as risk-free and secure as possible. It would be as commonplace to have high-speed internet and mobile banking as it is to have electricity. All of these government activities would need the gathering and utilisation of an individual's personal data, not just by the State but also by non-state actors. In the absence of legislation and infrastructure that are appropriate for the situation, a person would be put in a vulnerable position as a result of this, which would directly impact his right to privacy.

Internet of Things (IoT)

The Internet of Things, sometimes known as IoT, is a relatively new development in cyberspace that may be conceptualised as an interaction between computer software, telecommunication networks, and electrical devices. IoT is defined as a seamless linked network of embedded objects/devices, with identifiers, in which communication without any human intervention is feasible utilising communication protocols; however, mobile phones, tablets, and personal computers are not considered to be a component of IoT. This definition can be found in the "IoT Policy Document" published by the Government of India. In the broadest sense, the Internet of Things (IoT) is a network of devices that are capable of connecting to the web and turning ordinary machines into smart ones. For instance, if a coffee maker is connected to a smart phone, then all it takes is a tap on the smart phone for the coffee maker to begin brewing coffee. Another illustration of this would be the utilisation of a global positioning system (GPS) in a vehicle, which, since it is connected to the internet, enables the driver to navigate the route without the use of a map. In the Internet of Things, a smart refrigerator equipped with sensors will know more about an individual's eating habits than the individual's primary care physician. The intelligent refrigerator is able to recommend not only what should be cooked for the current meal but also what should be created for the future meal based on the ingredients that are now accessible in the kitchen. All of this is made possible by sensors that are built into the physical objects themselves. These sensors are able to detect and record data, which is then sent through the internet to intelligent servers. These servers then compile and sort the data before sending back intelligent solutions. Even when the wearer is asleep, an intelligent wrist band is able to detect high blood pressure. The man with high blood pressure would be roused from his sleep by a strong vibration from the wrist band. At the same time, the band would send all of the man's body vitals readings to a medical consultant, who would then analyse the data and send back any urgent emergency medication that was necessary. If necessary, an ambulance would also be dispatched to the man's home immediately and bring him to the hospital, where he would be treated in a timely manner. Through the utilisation of internet of things technology, a smart city is able to monitor and regulate on a much bigger scale the water supply, traffic, power, crowd control, and movements of people among other things. On the other hand, all of this raises the issue that an individual's right to privacy may be violated as a result of the recording of a great deal of data about his actions, with no assurance that this data would be protected by any safeguards. This information will be revealed as a result of this recording. The Internet of Things in India is expected to experience significant growth as a direct result of the government's ambition to digitally transform an initial 100 cities into smart cities. The Internet of Things is comprised of three separate stages: sensors for the gathering of data, a software application for the collection and analysis of data for decision making through the medium of the internet. The government believes that the most important stakeholders are the citizens, the government itself, and the industry; nevertheless, the foreign commercial entities that are participating must also be considered. This goal will have to be compromised since India is dependent on foreign technology and foreign investment in India in terms of technology, personnel, and money. The ambition of the government is to establish a connected and intelligent IoT-based system for our country's economy, society, environment, and global requirements; however, this vision will not be realised. Under these conditions, the government practically has no control over foreign organisations that operate in India for the purpose of pursuing economic profits without providing any assurance to the country's residents that their personal information will be protected. By utilising the internet, a significant amount of data would be gathered, and it would then be examined for the sake of decision making. This data is based on human actions and individual behaviour, which directly affects an individual's right to privacy. An individual's data can be captured, scanned, and analysed by numerous third parties in India and overseas, even without the individual's knowledge or agreement, and this can happen even when the individual is not participating in the activity or conduct in question.

Present legal framework and policies

The provisions of The Information Technology Act, 2000, which was enacted in the primary interest of facilitating e-commerce and Electronic Governance, gave only a very cursory treatment to the problem of protecting people's privacy in cyberspace. In the declaration of aims and reasons, it was said that there was a need to put in relevant revisions to support e-commerce. This necessity was mentioned. In addition, it said that there was an attempt to avoid misuse over transactions in electronic media and that civil and criminal responsibilities had been imposed for disobedience of the terms of the Information Technology Act. There were provisions for breaches of privacy and confidentiality included in Section 72. Provisions for the liability of intermediaries were included in Section 79, but only under specific conditions. It is against the law for civil courts to render a verdict on such a topic since, according to the Information Technology Act, an adjudication officer must be appointed instead. As a result, the problem of protecting users' privacy online was not adequately addressed. In order to adapt to the rapidly shifting landscape of online activity brought about by developments in technology, the Information Technology Amendment Act of 2008 was enacted and given official notice in 2009. New provisions were added to the modifications regarding data protection and privacy requirements, liability of intermediaries, government interception and monitoring, and the institutional structure for enforcement. According to the new provisions of Section 43A, if a body corporate that deals with sensitive personal data is negligent in ensuring that reasonable security practises and procedures are in place, and this negligence results in wrongful loss or gain for any person, then the body corporate in question will be obligated to pay damages to the person who has been negatively impacted. Any person, including an intermediary, who has secured access to any personal information and discloses such information to an unauthorised person in an unauthorised manner will be punished with imprisonment for three years or a fine of up to five lakhs rupees, or both, according to the new Section 72A, which states that such a person will be punished with imprisonment for three years or a fine of up to five lakhs rupees. A breach of a person's right to privacy in their private parts can now result in a sentence of up to three years in jail, a fine of up to two million rupees, or both, according to the new provisions of Section 66E. The newly added section 69A gives the government the authority to make directives that prevent the general public from accessing any material via any computer resource. If an intermediary does not comply with the directives given by the government, then that intermediary faces the possibility of being sentenced to seven years in jail in addition to a fine. The government now has the authority to permit the monitoring and collecting of traffic data or information for the purpose of ensuring cyber security according to the newly enacted section 69B. In the event that an intermediary does to comply with directives issued by the government, then such intermediary may be liable to a fine and imprisonment for a period of three years. The government now has the authority to establish the National Nodal agency in charge of Critical Information Infrastructure Protection thanks to the newly enacted section 70A. The protection of critical information infrastructure would fall under the purview of this nodal body, which would be responsible for all related actions, including research and development. The new section 70B gives the government the authority to establish the Indian Computer Emergency Response Team (ICERT), which would act as a nodal entity for the purposes of carrying out the tasks that are connected to maintaining cyber security. In accordance with the revised provisions of Section 48, the Central Government is required to establish one or more Cyber Appellate Tribunals, which would be responsible for hearing and deciding appeals lodged against the orders of the Controller or Adjudicating Officer. The Ministry of Electronics and Information Technology of the Government of India drafted a number of rules, some of which are as follows, in response to increased public awareness of activities in cyberspace and concerns over individuals' right to privacy:

(i) The Information Technology (Procedure and Safeguards for Interception, Monitoring, and Decryption of Information) Rules, 2009[14] are a set of regulations regarding information technology. wherein the competent power to order interception, monitoring, etc. resides at the level of a Secretary level official at either the Union or the State level, and such directives must be communicated to the Review committee within seven days. This committee will convene at least once every two months.

(ii) Any individual can send a request to the Nodal officer, who will then forward it to the Designated officer in accordance with the Information Technology (Procedure and Safeguards for Blocking Access of Information by Public), Rules, 2009, according to which the designated officer for ordering the blocking of any website must have a rank that is not lower than that of the Joint Secretary of the Government of India.

(iii) The Information Technology (Procedure and Safeguard for Monitoring and Collecting of Traffic Data or Information) Rules, 2009, which stipulates that the competent authority is the Secretary to the Government of India in the Department of Information Technology.

(iv) The Information Technology (Reasonable Security Practises and procedures and Sensitive Personal Data or Information) Rules, 2011 stipulate that sensitive personal data or information includes things like a person's password, their financial information, their physical or mental health condition, their sexual orientation, their medical records and history, and their biometric information.

(v) Guidelines for Cyber Cafés Under the Information Technology (Guidelines), Rules of 2011,wherein a cyber café must be registered with a unique registration number, user identities must be formed, and records must be preserved for a period of one year; all computers must be outfitted with software that is commercially accessible for safety or filtering purposes.

(vi) The Information Technology (Intermediaries Guidelines) Rules, 2011 provide that intermediaries must practise appropriate levels of due diligence.

Planning Commission, Government of India, on October 16, 2012, constituted Group of Experts, under the chairmanship of Justice AP Shah, Former Chief Justice, Delhi High Court, and vide it's report of ninety one pages proposed a framework for the protection of privacy concerns to serve as a conceptual foundation for legislation protecting privacy. This framework was proposed to serve as a conceptual foundation for legislation protecting privacy. This report has not yet been carried out in its entirety. National Cyber Security Policy -2013 was published by the Government of India's Ministry of Electronics and Information Technology (MeitY). It is a nine-page document that lays out a vision for cyber security along with a set of sustained and coordinated tactics for its execution. This policy not only provides an overview of what it takes to properly safeguard information, information systems, and information networks, but it also provides an insight into the method and strategy that the government is using for protecting cyberspace in the country. The legislative and executive branches have not yet finished putting this regulation into effect in its entirety. Recently, in the year 2017, the government began the process of reviewing the entirety of the field of data protection by establishing the Srikrishna committee, which was chaired by Justice B N Srikrishna, a former judge of the Supreme Court of India. The government asked the Srikrishna committee to investigate various issues relating to data protection in India and to give its recommendations. In November 2017, the committee issued a white paper in which it called on various stakeholders to discuss and debate a variety of problems in order to guarantee the expansion of the digital economy while maintaining the privacy and protection of individuals' personal data. A very effective statutory authority that also possessed regulatory capabilities was proposed in the study.

CONCLUSION

There are significant efforts being made to digitally empower India; yet, this comes with increased online hazards due to the fact that facilities connected to the internet might be brought down by antisocial forces for which there are no proper defences available.The Internet of things and the Digital India initiative will lead to an increase in dependency on the usage of cyberspace, whether through the internet or other gadgets. This will further expose an individual's life to the risk of having their online privacy violated. Therefore, protecting one's privacy while using the internet will become an even more pressing concern in the years to come. The maintenance of a delicate equilibrium between state obligations for national security, economic and social issues, and the online privacy of the individual is necessary in order to achieve the goal of a safe and secure cyberspace. Because almost every digitisation project, irrespective of the industry, requires a network connection and may therefore be faced with a cyber security problem, security and privacy concerns need to be taken into consideration right from the beginning of the project design stage. New approaches for the construction of digital systems should be extensively adopted by developers, in particular through the implementation of a safety, security, and privacy-by-design approach. Infrastructure operators need to make sure they have a technology management competence, especially if they want to reduce their reliance on a single technology supplier in a global setting through the use of multi-vendor architectures and federated service structures. Any newly produced technology has the potential to either be employed in an ethical manner in accordance with the goal for which it was originally designed or for other, less ethical goals. Because cybercriminals are typically early adopters of new technologies like artificial intelligence, the internet of things, and quantum computers, and make use of them in a manner that is patently immoral, RTOs and industry need to collaborate in order to solve this issue through the application of suitable research initiatives.

REFERENCES

1. E. J. Bloustein, N. J. Pallone, Individual and Group Privacy, Routledge, New York, 2017.
2. M. Oostveen, U. Irion, The golden age of personal data: How to regulate an enabling fundamental right?, in Personal Data in Competition, Consumer Protection and Intellectual Property Law (eds. M. Bakhoum, B. Conde Gallego, M. O. Mackenrodt, G. Surblytė-Namavičienė), Springer, (2018), 7–26. Available from: https://link.springer.com/chapter/10.1007/978-3-662-57646-5_2.
3. R. Romansky, A survey of digital world opportunities and challenges for user’s privacy, Int. J. Inform. Technol. Secur., 9 (2017), 97–112.
4. J. J. Hanus, H. G. Relyea, A policy assessment of the privacy act of 1974, Am. Univ. Law Rev., 25 (1976), 555.
5. M. Shabani, P. Borry, Rules for processing genetic data for research purposes in view of the new EU general data protection regulation, Eur. J. Human Genet., 26 (2018), 149–156.
6. A. V. Tsaregorodtsev, O. Ja. Kravets, O. N. Choporov, A. N. Zelenina, Information security risk estimation for cloud infrastructure, Int. J. Inform. Technol. Secur., 10 (2018), 67–76.
7. O. Yu. Zaslavskaya, l. A. Zaslavskiy, V. E. Bolnokin, O. Ja. Kravets, Features of ensuring information security when using cloud technologies in educational institutions, Int. J. Inform. Technol. Secur., 10 (2018), 93–102.
8. P. Wandra, H. Jie, DeepProfile: Finding fake profile in online social network using dynamic CNN, J. Inform. Secur. Appl., 52 (2020), article 102465. Available from: https://www.sciencedirect.com/science/article/abs/pii/S2214212619303801.
9. V. Kharchenko, Big Data and Internet of Things for safety critical applications: Challenges, methodology and industry cases, Int. J. Inform. Technol. Secur., 10 (2018), 3–16.

10. I. Alsmadi, R. Burdwell, A. Aleroud, A. Wahbeh, M. Al-Qudah, A. Al-Omari, Introduction to information security, in Practical Information Security (eds. I. Alsmadi, R. Burdwell, A. Aleroud, A. Wahbeh, M. Al-Qudah, A. Al-Omari), Springer, (2018), 1–16. Available from: https://www.springer.com/gp/book/9783319721187.
11. H. Paanen, M. Lapke, M. Siponen, State of the art in information security policy development. Comp. Secur., 88 (2020), article 101608. Available from: https://www.sciencedirect.com/science/article/pii/S0167404818313002.
12. M. A. Ferrag, H. Janicke, Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study, J. Inform. Secur. Appl., 50 (2020), article 102418. Available from: https://www.sciencedirect.com/science/article/pii/S2214212619305046.
13. A. R. Mahlous, SSR: A framework for a secure software reuse, Int. J. Inform. Technol. Secur., 10 (2018), 87–98.
14. Y. A. Ivanova, Assessment of the probability of cyberattacks on Transport Management Systems, Int. J. Inform. Technol. Secur., 10 (2018), 99–106.