IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.116111

Survey On Digital Security Versus Private Information

Pragati Giradkar[1], Neehal B. Jiwane[2], Ashish.B. Deharkar[3]

Student, Computer Science & Engineering, Shri Sai College of Engineering & Technology, Bhadrawati, India[1]

Asst.Prof, Computer Science & Engineering, Shri Sai College of Engineering & Technology, Bhadrawati, India[2]

Asst.Prof, Computer Science & Engineering, Shri Sai College of Engineering & Technology, Bhadrawati, India[3]

Abstract*:* This paper demonstrates digital security vs. private information. Digital security will be considered a world security agenda that will concern protecting states and citizens from the misuse of sensitive information. By using privacy and security measures, a corporation can manage the protection threats related to it. Moreover, it is a significant a part of the organization because it prevents financial and reputational damage for any organization. This report aimed to know the small print of digital security and also the issue associated with the identical in terms of handling private information. It sets the objectives and background to the study within the introduction section. It then went on to research the methodology section. a combination of primary and secondary research was employed in this project, using survey and thematic analysis. The research paper then collected data and analysed the identical with the assistance of MS Excel graphs and charts and peer-reviewed journals and articles. This report is ready to satisfy the digital economy and manage the digital security and privacy risk for various organizations' social and economic prosperity. This paper discusses the critical dimensional areas towards digital security to attach with the digital environment and privacy of the knowledge technologies. This paper has been articulated risk management by analysing the possible threat areas to comprehend the present situation. It came up with the knowledge that digital security has the prospect of causing significant issues while storing and securing private information.

Keywords*:* Digital security, encryption, RFID, risk assessment.

I. INTRODUCTION

The process of developing digital security has become an enormous necessity in recent times. the foremost reason for this lies within the overuse of technology in every aspect of companies . this will be mainly because current cybercrime and attacks have made headlines which will jeopardize ordinary people's trust in sharing information online. This project research shall consider the identical. First, it Should set the objectives and also background of study. Second, it shall also discuss the literature review and thus the methodology for conducting the research. Finally, it shall conduct and analyze data.

Problem Statement

The problem statement of the project associates with this concept of digital security and therefore the storage of the personal information in companies also analyzing the risks of the identical in digital security.

Objectives

To analyze digital security issues in companies • To explore the threats to the personal information management • To evaluate the failure of digital security to guard private information • To come up with the strategy for mitigating the risks.

Research Background

The background of the study is related to the concept of digital security for the private information shared on the digital platform. The concept of digital security may be a collective term describing the main points of the resources employed for shielding the web identity, data, and other assets. These tools might include web services, software, smartphones, SIM cards, secured personal devices, and biometrics the first purpose is to secure the web and digital identity and presence of the individuals. the employment of digital security measures has generated growing significantly since the net and digital presence of people is more important than their offline presence. additionally, the rise in cybercrime and attacks has increased the measures of cybersecurity. However, the difference between digital and cybersecurity can be considered. While the previous involves protecting the net presence, the latter covers more grounds, including entire networks, computer systems, and other digital components. Therefore, cyber protection and security are more complex and

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022
DOI: 10.17148/IJARCCE.2022.116111

challenging jobs than digital security protection Companies use the identical with the assistance of assorted steps and measures. They ensure to appear after the generation of awareness among the staff regarding the need for this security.

Research Rationally

Companies are taking a growing interest in incorporating digital techniques for the expansion and development of their businesses. during this regard, they need the role of undertaking the desired measures to avoid the probabilities of risks and threats within their businesses within the long term . the utilization of digital security measures can be helpful for the businesses to manage and secure the digital and online identities of both employers and employees working for the businesses. they're also capable of protecting the knowledge of the purchasers shared online.

Therefore, the selection of the scientific research could be helpful for the business owners getting to install digital security within their operations. the event of the general digital security systems can be an extended and sophisticated process. Moreover, it's different for each company. Thus, company owners might have the benefit of the study by analysing the assorted strategies essential in digital security. they may come to be told about the ways and means of developing the settings of digital security. they could also find out about the risks and threats of digital security in protecting private information in employees and customers and taking precautions against it.

II. LITERATURE REVIEW

Introduction

Privacy and security are interrelated with one another. Privacy is related to any quite right which can control some personal information. Privacy will be maintained by using several privacy policies associated with any organization . On the opposite hand, security means how any organization can protect the knowledge. Digital security and privacy policy is considered the priority of various public policies within the era of a data-dependent economy. the most challenge of business, government, and other organizations are to manage the risks associated with the private information of any organization. A brief overview of digital security and personal information are going to be discussed . After that, it'll discuss associated risks and mitigating procedures of these risks. Then, it'll examine the evaluation of the failure of digital security, followed by the literature gap Different types of digital security are seen during this digital world which is offering a large choice for the defence method such that

Digital security is that the concept because the collective term for describing the resources must employ for shielding online data, identity, and other such vital assets. However, this tool is related to antivirus, secure personal devices, web services, and biometrics . Digital security is that the process of protecting online identity. Digital security is crucial to trust during this digital age. Within this environment, digital security is that the policy and framework that proved the essential and practical principles to deal with without restricting use, the openness of digital.

Technology, also the dynamic nature without inhibiting the potential to foster innovation to be on the social technologies. Moreover, privacy and security are associated with one another. Privacy relates to the rights for controlling the non-public information for a way to use. These two aspects of security and privacy overlap within the connected world. in line with the literature, it's been seen over the industry to differentiate these two concepts. However, privacy, similarly as security, must need to be maintained. Organizations use the customer's private information to marinate the database for the operations and supply the services and products. Therefore, they have to be focused on protecting those data. Different types of digital security are seen during this digital world which is offering a large choice for the defense method such that

- Current and updated firewall: firewall is taken into account because the network device which will monitor the packets going out and into the blocks and networks or by allowing them accordingly. However, it's been set for outlining the permissible traffics . additionally, the firewalls must be updated to confirm digital security. Hence, it's been wont to protect the knowledge system within this organization's database to reinforce the activation of services appropriately.
- Antivirus software: Viruses will be delivered by malware and another malicious system wont to infect the organization data and produce the system towards the screening halt. However, an antivirus detects and uses for cleaning all those infections to stay out the suspicious aspects regarding securing the private information and isolates those likely threats.
- Remote monitoring software: Remote monitoring may allow the information security team to gather the information; oversee all the hardware and applications by diagnosing problems remotely . However, remote monitoring software provides the conveniences and adaptability to enable the administrators to resolve those implications from anywhere.
- Proxies: proxies are commonly referred to as the digital security tool that may bridge the gap between the web and users while using the rule to filter in line with those organizations' information technology policies. However, proxies

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022
DOI: 10.17148/IJARCCE.2022.116111

block those dangerous websites and leverage the possible authentication system to manage the access and monitor the usage. additionally, this server generally acts because the web filter and firewall to attach the shared network and caching the information to spice up up the quality request.

- Vulnerability scanner: A vulnerability scanner could be a concept for inspection to the potential points that may exploit the pc network for identifying the protection holes. However, vulnerability has been wont to classify and detect a system's weakness in a very computer, installation, and networks and predict countermeasure effectiveness . The organization system may use this tool for evaluating, detecting, and managing that weakness. the knowledge technology security team may use.
- Associated Risks According to the literature, a digital security risk is an occasion and action that will damage constituent, software, and personal data or information within the organizations. Understanding all the present digital security may help design the right decisive mitigation plan regarding the protection risk . However, any size of business both small and more prominent has been exposed with several digital risks can cause some damage for the event of business or organizations. Here a number of the digital risks that are related to the enterprises or businesses are discussed below- • Data risk: however, data is worried with thriving the engine. Those are knowledge-based economies for operating the industry or business; management must make sure that the business data is stored in safe hands . However, the chance of knowledge is related to the misuse of sensitive business data and essential customer data.
- Cybersecurity risk: while connecting with the web for business, there's no possible thanks to eliminate this risk. this sort of risk is evolving intuitively and rapidly; however, the foremost common cyber risks are ransomware, DDOS attack, and compromised network.
- Reputational risks: company valuation has been decreasing significantly for selling out the version of business. the corporate has to consider the reputational risk for creating a well-revised plan for avoiding or accepting the risks. Reputation-based security is that the security mechanism which will classify all the essential files supported the security of the inherently garnered reputations to those organizations. However, this could make it possible by identifying and predicting the security of the files supported the widespread use towards the wide community users.
- Talent storage and cultural risk: the dearth of a skilful workforce can weigh down the business growth from the expected level. The organization should need to hire a talented or knowledgeable team to support the present projects. Even corporate culture includes a significant impact on the success of the digital security plan. Organization culture has been related to the values, beliefs, and attitude may drive the team member behaviours while protecting and defending the organization of business from vulnerable attacks. Though work culture is often changing, those are opting towards the short-term role of contract or freelancing.
- Privacy risk: while storing personally identifiable information for business purposes, the protection team must have this process in situ by describing it correctly, storing it, and securing the identifiable information personally collected from several users or customers. The organization should must observe the privacy laws by describing how they must handle sensitive personal information.
- Third-party risk: third party risk is taken into account because the potential threat of the digital security concept those are presented to the staff of the organization or sensitive customer data, organization process or operation, and financial information . These are from the organization's supply chain and therefore the other outside parties providing services and their products and having access to the privileged system. Regulatory and violations are intensified globally, and reputational damage, systemic events, and financial dependence are related to this type of risk.
- Technology risk: this sort of risk is potential for any failure regarding the technological aspects to disrupt the business. However, companies face many various sorts of technological risks related to cyberattacks, service outages, password theft, SQL injections, and more. Software defects, floods at the middle of knowledge, and tripping over the ability cords are considered the technical risk related to the digital risk to the info or application for the knowledge technology that harms the business operations. • Artificial intelligence risk: it's one among the many digital security risks that the researcher has identified. Towards the substitute system, this sort of risk is that the potential of the adversaries while compromising the integrity of the method of deciding . Therefore, it should not make the alternatives that the designer has been expected or desired. • Compliance's risk: security compliances are generally supported the need of external sources instead of objective to risk management of own organization business. However, the compliance risk is related to the meeting of assorted controls for shielding the integrity, confidentiality, and availability of essential data. additionally, this type of risk is handling the environmental damage and pollutions of the operation of organizations. Mitigation Procedure Here, many digital security risk has been discussed those are related to the non-public information. to make sure organizational security in digital aspects, there are many mitigation strategies are developed below.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022

DOI: 10.17148/IJARCCE.2022.116111

- Identifying the key assets: the organization should maintain its strategies to mitigate all those challenging risks. However, implementing the governance risks and also the strategy to the compliances can be helpful that may be defined because the organizational approaches across the simplest three critical practices of the governance, compliances, and risk management. to properly manage the digital risks, the corporate should identify the organization's critical assets . First, however, puzzling over the possible ways in which could be exposed as vulnerable threats. Moreover, this identification is that the key asset for successfully identifying the vulnerabilities and nature of potential attacks.

III. EVALUATION OF THE FAILURE OF DIGITAL SECURITY

According to Chen et al. one among the numerous issues cybersecurity leaders face is that the costs of some significant incidents to other stakeholders within their organization. Some elements may have a straight impact, like costs related to replacing physical IT assets or loss of revenue from their business activities which can not be established during the outage . Nevertheless, others are challenging to ascertain. Companies are didn't implement digital security because they're not determining their effectiveness. it's been seen that 80% of the organizations did not include business users in cybersecurity purchase decisions. they are doing not include any high-powered committee to guage the business impact and risks associated with cybersecurity investments. Third-party organizations may perform detailed investments in cybersecurity technologies without measuring the effectiveness of these technologies. 80% of companies fail to speak with business stakeholders regarding cybersecurity issues .

According to Ioane, Kibbes, and Tudor , it's been observed that two-third of the cyber-attacks may target small and medium-scale organizations. It happens because hackers often exploit smaller organizations with a scarcity of resources to go looking for data shared with large organizations. Digital security efforts are often measured by using Security Benchmark Index Survey . It provides a close overview regarding the protection benchmark index of a company. This index helps the organizations to live their position compared to their peers. By using their free and in-depth resources, companies can protect their critical systems and sensitive information. For assessing the digital security of any organization, a risk assessment has to be done. Then, they have to gather different forms of information regarding their digital security policies and procedure of maintaining security to the pc systems, computer networks, email, and far other software . After that, they have to spot and document different internal and external threats. it should involve several tactics, techniques, and procedures used for several target organizations. For assessing the vulnerabilities, they will use different tools by which they'll scan their networks and determine what services they're executing. According to Kumar and Roy , it helps to test whether there's any updated software available within the organization and explore for well-known vulnerabilities. The IT administrator may use several tools to execute the pre-defined vulnerabilities against a selected system and use brute force attacks against the end-users . they will appoint a security specialist to live the resilience of the organization by using penetration testing. After that, they have to perform business impact analysis to work out several impacts of various consequences of digital security threats. Consequences will be financial, operational, and reputational. they have to form a business continuity plan or resilience plan . they have to have a transparent picture regarding costs related to the failures of IT or in business operations. After getting a transparent idea regarding the potential impact of digital security, they'll prioritize resolving the immediate flaws in cybersecurity attacks. If the corporate authority must make some changes to the system security, they have to check these to test whether or not they negatively impact other systems. because the staff is considered the foremost security liability, they have to make sure several rules and regulations to perform documented policies of the organization. they have to supply regular education to the staff, which may be wont to perform their business process.

IV. LITERATURE

After evaluating all the research papers and peer-reviewed journals, it's been found that the majority of the researchers have done theoretical research on the digital security and privacy of data. However, they are doing not provide any detailed discussion regarding any practical work about any organization's digital security and privacy . This research work doesn't provide a close overview of the chance analysis about different digital security threats of any organization. Further, it doesn't offer an in depth overview of the business continuity plan and disaster recovery decide to mitigate the risks of digital security and privacy of knowledge.

V. METHODOLOGY

Research Onion

METHODOLOGY secondary sources of research and data collection. the first research section shall specialize in a quantitative survey. during this regard, the researcher shall prepare a questionnaire and target people working in companies to investigate their experience on Various steps and stages of research can be mandatory while completing the identical. during this regard, the research onion by Saunders helps understand the varied stages and layers of a pursuit

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022
DOI: 10.17148/IJARCCE.2022.116111

project . the method is comparable the peeling of the assorted layers of an onion. While peeling these layers, the researcher comes across the philosophy, strategy, approach, and research. aside from this, the researcher is additionally required to specify the processes of information collection, sampling, data analysis, time horizon, etc. These are essential parts of the onion.

Research Philosophy

This is an integral a part of the scientific research. It enables the researcher to judge the character, source, and sources of developing data and knowledge regarding the subject. Pragmatism, positivism, realism, and interpretivism are the four sorts of research philosophy types. This research shall concentrate on the positivism research philosophy. The advantage of using this philosophy includes the flexibility of the researcher to incline to factual data and reliable sources while conducting the research. However, this sort of philosophy often restricts the role of the researcher in data collection, which could be a limitation.

Research Approach

This is another vital a part of the scientific research and includes all the steps to form broad assumptions about narrowing down the arguments and deductions regarding the identical. Three differing types of research approaches are commonly used, including deductive, abductive and inductive approaches. The deductive approach of research shall air focus during this project . this kind of approach is commonly helpful in forming casual bonds between concepts and variables, which could form a bonus for the research. However, it'd be an obstacle since it tends to generalize the findings and analysis of the research.

Research Design

This a part of the research is mandatory for analysing the main points of the whole strategy of the researcher and also the logical plan for collecting data and analysing them for achieving the deliverables. Exploratory and conclusive designs are the 2 varieties of research designs. the look utilized in this research is that of the descriptive sort of the conclusive research design . This may be advantageous since it takes time to investigate the research for determining the variables related to the identical. The drawbacks of this design can be observed within the kind of the lack of the study to investigate and verify the results with statistics.

Data Collection

The process of collecting data is that the most crucial a part of the research. This project shall combine both primary and digital security. The secondary research section shall concentrate on thematic analysis. The researcher shall break the research topic into several themes and analyse their impact on digital security. the information analysis shall be made supported the gathering using both qualitative and quantitative sources of knowledge.

Sample Technique

The sampling technique is again a necessary a part of the expansion and development of research. this is often mainly because it's concerned with targeting a particular population within the completion of the research. For this project, the researcher shall use a sampling technique using the probability method. For the quantitative survey, the questionnaire shall be presented to about 100 employees coping with digital security. On the opposite hand, the researcher shall analyse four themes to grasp the main points of the assorted attributes and elements of the research topic.

Data Analysis

This is the ultimate and most important section of the scientific research. The researcher tries to research and discuss the collected data to develop accurate results against the identical. within the primary section, the researcher can generate the participants' opinions against the questionnaire. The analysis shall be through with the assistance of MS Excel graphs and bars. The researcher shall attempt to analyse the importance of their opinions supported the bulk answers. Further, the researcher shall use scholarly and peer- reviewed journals and articles for analysing the main points of the varied themes and discuss their deductions.

Ethical Considerations

The use of ethics and morality could be a significant necessity while completing any research work or project. The researchers must follow a selected sort of considerations during this regard. as an example, they could follow the info Protection Act of the united kingdom . Following this, they'd should make sure that they're securing the knowledge present online. they need the role of avoiding the probabilities of manhandling the knowledge of the participants while keeping their identities anonymous. Furthermore, they have to make sure that the collected data and data are secure on the digital platform by blocking external sources from accessing the identical.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022
DOI: 10.17148/IJARCCE.2022.116111

VI. THEMATIC ANALYSIS

Theme 1: Digital security issues in companies Digital security is crucial within the companies to assemble, securely store and adequately protect user or employees, customer data, and proprietary secrets. it has been analyzed that dangerous damage of the company's brand and reducing the quality of the merchandise for his or her produces for getting the proper revenue and profitability of the business . However, digital security is that the critical business function to stay up personal information. However, non-core competencies remain for boards with a serious number. Therefore, researchers are suggesting not reporting directly regarding these aspects of digital security to the company's CEO and reducing effectiveness. According to the thematic analysis, digital security is not just a technological issue about having the most recent and advanced security software. it's considered the foremost significant vulnerability and also the potential best defence . Most of the companies from different sectors would have regarding this cybercrime that laid within the regular practices and awareness of their companies employees. Researchers know the majority within the firms are conscious of those vulnerabilities and develop the approaches and processes to make absolute to not fall victim to digital criminals. Apart from that, attacks are still occurring over those firms using more advanced security, unfortunately, and even successfully by those attackers. However, it has been analysed that law firms usually have such insurance to safeguard their customer's financial losses . Cybercrimes happen due to the reason for money where most of the rich clients are associated. whether or not recovering the cash eventually, stress and impact are involved that's a serious accident for destroying the organization brand value or reputation. Moreover, the organization be focused on digital security to secure the private information associated with the high amount of value.

Theme 2: Ways of handling private information Companies usually have the role of handling the bulk of non-public information. These might belong to employers, employees, and customers. They, therefore, have the role of handling and maintaining the identical. the event of the protection settings is critical for managing and handling private information within the professional sector . they fight to prioritize steer and build their security settings against the identical. as an example, the customers' payment and online banking information are going to be more valuable than the identities and credentials of the workers. They, therefore, must prioritize the identical. Companies naturally have an additional responsibility after they're attempting to shield private information. they need to create sure that they conduct a risk assessment to avoid data theft and security issues. They further attempt to monitor the data and thus the activities of the staff in handling the identical . If they find any discrepancies with handling the data and knowledge, they need to handle the identical by securing their private information. Finally, the authorities check the progress in data security and management within their services. they need to avoid dissatisfying the consumers by showing discrepancies with their data and data.

Theme 3: Risks and threats with digital security Several risks and threats might occur while operating digital security systems. this can be often mainly because the individuals conducting cyber-attacks are more powerful and prepared than the digital tools employed in securing data and identity online. as an example, they may face the matter of ransomware . this might occur as a spread of malware or malicious software attempting to encrypt the data and data of the company. They extort for releasing unlock code. Most of such ransomware is delivered with the help of emails. Phishing is another type of risk in digital security systems. it's a trial to come back up with sensitive data while posing as a trustworthy contact. This might occur when a hacker site uses the logo and data of a company to look as a link to the consumers. they supply similar visuals, and customers might provide their payment credentials during this, generating a cyber-attack . the event of the overall concept of hacking is also a major threat to digital security. this can be often mainly because when individuals gain access to the IT systems of a company from the skin. they struggle to access the databases and gain the Mastercard credentials of the purchasers. this might be an enormous blow to the digital security settings of the company.

Theme 4: Mitigation strategies for the risks Companies have the role of bobbing up with effective strategies for mitigating these risks and threats. they need to create sure that they know the risks and threats possible within the digital security systems. they need to rent IT professionals and train their employees in advanced IT lessons to help them understand the little print of managing security risks . The owners must strengthen the IT department and enable them to look at the exercises of the numerous departments to verify that they stand back from chances of security issues. They also must enhance the investment in IT and acquire more tools and software for preventing malware attacks. Updating the software and tools is another strategy. This might enable companies to avoid using outdated tools. They also must confirm the endpoint protection of their networks remotely bridged to the devices. the use of firewalls and antivirus tools might help prevent variety of the foremost common forms of cyberattacks . Recently, the employment of proper storage and backup systems has gained popularity. Companies might use cloud storage settings to remain their data and knowledge protected online. they need to have control access to all or any or any the systems and monitor the activities of the staff within the identical.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 6, June 2022
DOI: 10.17148/IJARCCE.2022.116111

VII. CONCLUSION

In this paper, digital security versus private information is discussed in an exceedingly detailed format. It provides an in depth overview regarding digital security and also the private information of any organization. This report provides a transparent idea regarding several mitigation strategies for the identified risks of digital security. Organizations must help cybersecurity professionals resolve or mitigate the risks related to digital security. it's been observed from this paper that the majority of the work is completed in theoretical format. However, it doesn't provide any idea about several practical implications of digital securities in society. Implementation of a digital security policy helps any organization combat the cybersecurity threats related to them. it should cause significant changes regarding the competitive environment of the organizations. Legal regulations play an important role in maintaining cybersecurity standards within any organization. The governments implement legal regulations to safeguard the privacy-related information of a personal or any organization. the most aim of those acts is to scale back the possibilities of cybercrime occurring by using digital devices. To ensure privacy, hacking is taken into account an criminal activity. The person involved during this crime are going to be punished. frequency Identification can even be implemented for maintaining IT security within any organization. It is used for asset tracking, people tracking, inventory detection, and plenty of others. For this case, a centralized system are often deployed for controlling and transactional operations. It provides real-time operations for maintaining the digital security of any organization. It also provides secure access to a selected space while keeping a record of the user. they have encryption standards for maintaining information security within the organization. Encryption helps to boost the protection feature of any organization and use to stay the sensitive on the QT format. Many security algorithms are introduced and should be employed by several companies during this world. Most of the safety algorithms are associated with ASCII text. only a few algorithms can handle UNICODE text. Nevertheless, within the digital world, UNICODE plays an important role in data communication. This paper provides a close overview regarding the evaluation of the failure of digital security.

REFERENCES

[1]. Lowlesh Nandkishor Yadav "Predictive Acknowledgement using TRE System to reduce cost and Bandwidth" Factor 7.39 Vol. 11, Issue 3, March 2022.
[2]. Ashish B Deharkar "An Approach To Reducing Cloud Cost And Bandwidth Using Tre System"
[3]. Hunter, J.F., (2017). Is your smartphone a digital securityblanket? The influence of phone use and availability on psychological and physiological responses to social exclusion.University of California, Irvine.
[4]. Grimm, J., Koehler, K., Lust, E.M., Saliba, I. & Schierenbeck, I., (2020). Safer field research in the socialsciences: A guide to human and digital security in hostile environments. Sage.
[5]. Salminen, M., (2018). 2.10 Digital security in the BarentsRegion. Society, environment and human security in the ArcticBarents Region, p.187.
[6]. Bosma, E., (2019). Multi-sited ethnography of digital security technologies. Secrecy and Methods in Security Research: A Guide to Qualitative Fieldwork. New York: Routledge, pp.193-21