Challenges of Information Security in the Contemporary Cyber Threat Perception

Tripti Misra, Kingshuk Srivastava, Rajeshwari

Abstract*: *Information security comprises advancements, methods and practices proposed to guarantee protection of system hubs, programs, information, data and system from hack assaults, modifications to data or unintended access. To repress cybercriminals from gaining access to system resources specifically sensitive data, it is fundamental for organizations and individuals to take necessary actions to preserve the confidentiality, integrity and availability of delicate data. Information security spreads complex strategies to safeguard not only data during transmission, but also data stored in the system even when the system is not connected to the internet. In other words, it encompasses security of both data at rest and data in transmission. Numerous strategies have been employed by the professionals to protect organizations and records from interlopers. To deal with malevolent projects, there are a great deal of "off the rack" just as tweaked items accessible in the market which additionally give ongoing barrier and security to the delicate and sensitive data. There is still absence of techniques on the most capable strategy to appear and execute tasks that can be accustomed to the activities taking place at real time. This paper focuses on looking into the present methodologies used to give digital security, and identify the various loopholes in the present situation.

Index Terms*: *artificial intelligence, bot, cyber security, proactive.

I. INTRODUCTION

In the modern world, everyone's life is moving towards digitalization and dependence on digital media is an ever-increasing phenomenon. This is the time where one can discover everything on web, be it business, preparing on specific subject/course, busing and selling of goods or services, or setting aside cash through trades' comparisons. With everything connected through Internet currently, comes the hazard related with them. In the contemporary world, the quantity of data that we share over Internet has additionally intensified by a wide margin. The information is not any more constrained to just one individual, lone system yet it goes from a single location to other through network. With this quick spread of information amongst various frameworks and systems, occurs the necessity to verify information from getting under the control of pernicious clients. An individual requires to ensure that both the information in still state and information in movement as information security has turned out to be the utmost requirement. Contemporary web is one of the fundamental and quickly rising components for progression of industry. Industry 3.0[1] is being used as the greatest correspondence and information exchange means at present. Web and billions of adaptable and related devices immediately overhauled correspondence mode. Artificial Intelligence has replaced individuals by automating various activities in numerous application areas. Sensitive data related with an individual is being stolen and likewise, people who are using Internet are falling prey to various leveled threats. Delicate information stowed in "Mission-Critical" applications utilized in medical clinics, airports, railways, enterprises and even the banks are the focal points for being stolen these days, with the huge usage of web. Digital security is transforming into a troublesome issue for the entire world by means of intruders attacking individuals or organizations with the motive to gain access to their personal details.

The internet intruders are encountering a changeover with the growing availability of information transmission, related devices, and sensibly valued hacking apparatuses that empower them to dispatch evermore astounding and solid ambushes against an Information Security specialist's organization. The risk to digital security is spiraling at a gigantic speed. Advanced transgressions are expanding a result of the nonattendance of appropriate digital safety efforts just as law of land. Digital Security in Industry 3.0[1] contains frameworks that react simply after a rupture has happened which is responsive in nature. This deduces that frameworks have been succeeding freely, or by teaming up with individuals in making a customer orchestrated creation field that can assemble data, analyze it, and summon activity upon it. A great deal of research has been completed to verify information, framework, arrange, and so forth from awful clients. This paper is an endeavor to take a gander at the various looks into that have been done in the different areas of Cyber Security in the whole world.

II. EVOLUTION OF CYBER SECURITY

Cyber security has continued to evolve with each passing generation [2]:-

A. Generation I

It all started in late 1980s. There were typical Virus attacks on stand-alone PC's that affected the

Revised Manuscript Received on July 22, 2019.

Tripti Misra, School of Computer Science, University of Petroleum and Energy Studies (UPES), Dehradun, India, tripti.misra@ddn.upes.ac.in
Dr. Kingshuk Srivastava, School of Computer Science (SCS), University of Petroleum and Energy Studies (UPES), Dehradun, India.
Prof. Rajeshwari, School of Business, University of Petroleum and Energy Studies (UPES), Dehradun, India. tripti.misra@ddn.upes.ac.in

businesses. They tried to track the proliferation of unlicensed software. Because of which, anti-virus products were necessitated.

B. Generation II

In Mid 1990s, as the internet started becoming key to the businesses and individual's lives, hackers commenced to expand network by interacting among themselves, laying the base for cybercrime for monetary benefits. This led to the creation of first firewall, along with intrusion detection systems (IDS).

C. Generation III

During early 2000s, Fraudsters started examining networks and applications to assess and exploit vulnerabilities and threats in the IT organization. Anti-viruses, Firewalls, and intrusion detection system (IDS) were not efficient enough to fight these exploits. This gave rise to intrusion prevention systems (IPS).

D. Generation IV

Around 2010, cyberattacks extended from universal espionage to massive data breaches of individual to expansive scale internet disturbance. Assaults were concealed in everything from simple files to pictures—vague and polymorphic. However, Generation II and Generation III products were able to provide proper access control and analyze traffic but it lacked the capability to validate the content received by an individual through email. This sparked the need of anti-bots and sandboxes to address new and zero-day attacks.

E. Generation V

Near 2017, large-scale, multi-vector mega attacks that used advanced tools and technologies sparked a necessity for an integrated and unified security structures. This requires development of integrated architecture with proactive solutions that provides security from threats in real time, anticipating assaults on virtual environment, cloud storage, endpoints, remote workplaces, and mobile phones.

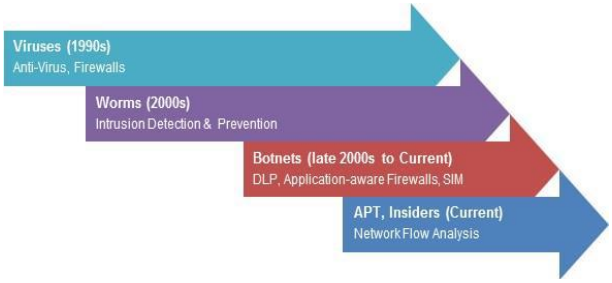

Fig. 1 Evolution of Cyber Security. Here APT* stands for Advanced Persistent Threat. [3]

III. IMPORTANCE AND IMPACT OF CYBER SECURITY

Digital security has remained a vital aspect consistently and it does not seem to be trifling in the future as well. At present the internet is ruling our worldwide market, the Internet of Things, can be a contingent issue in numerous occasions. Therefore, the digital safety apprehensions would no longer be an unforeseen factor in the years to come. Being cautious about the conditions, the internet professional's are devoting an ample amount of time and exertion in envisioning digital attack models.

The biggest challenge today is to secure data from malicious programs and people with iniquitous intensions. Until now, associations have utilized several methodologies to protect information from malicious users; however, all of them are responsive in nature. Reactive agents achieve their goals by enforcing an instinctive reaction, simply responding to modifications in their surroundings with allied actions. Reactive agents adjust in light of the progressions without reckoning future changes or thinking about the future effects of alteration. In other words, they wait for the systems to be attacked and later resolve to mitigate those attacks. Such agents lack decision-making capability for a new attack that might occur as it has been trained to appease current attack. It is no longer ok to just block and defend. In order to pacify the new attack on data, it requires new training on dataset, which might take time. Plenty of aspects shown in Fig. 2 depict the importance of Cyber Security in current and upcoming years [4]:

A. Sensitive Information

With abundant data available on internet globally, a lot of personal and critical information is compromised for defacement, humiliation, harassment, rumormongering and much more. There is a need to ensure security of such delicate information to evade its adverse influence in upcoming years.

B. New Vulnerabilities

A window is unlocked for new weaknesses and threats due to immense growth in the modern and new technologies. Attackers or hackers keep on trying hard to gain access to data leading to identification of new vulnerabilities. Organizations must evolve new methods and procedures to protect their data from such vulnerabilities.

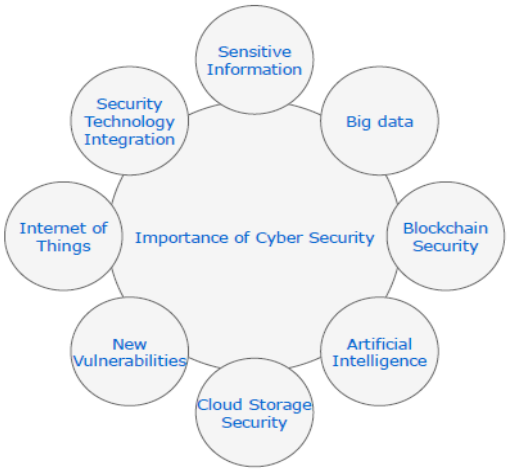

Fig. 2 Importance of Cyber Security

C. Big Data Security

The enterprises are handling data created every

second on internet. The data is in various types and formats. It can be structured or unstructured as well and securing both is a huge concern [5].

The lack of proper data analytics procedures can serious cyber security risks and issues to such big data. So it becomes significant to analyze data suitably and accurately in order to secure big data.

D. Cloud Storage Security

Enterprises nowadays depend largely upon cloud storage for data warehousing because of the tremendous amount of data being created every next second. Cloud storage [6], if not properly handled can lead to severe cyber security problems like breach of confidentiality, integrity and of course availability. Thus, it is a necessity to design a model for securing cloud storage in order to safeguard data from hack attacks.

E. Internet of Things [7]

The contemporary world is heavily relying on latest internet technologies for data access and transfer. Nevertheless, majority of them are not vigilant about the concealed issues associated with these technologies and are consuming the new age innovation without emphasizing much on wellbeing and safety. However, weaknesses related to individual information can be a genuine risk anticipating them. The utilization of imperfect strategies and default secret codes procedures would not prove to be great at last. Loopholes in security can be a principal digital security risk in the forthcoming year, also.

F. Blockchain Security

Blockchain [8] has demonstrated its capability for changing conventional industriousness with its prime attributes: devolution, persistence, obscurity as well as inspect ability. The potential outcomes of blockchain security can be an imperative marvel in this specific situation. This innovation in security, starting from exclusion of passwords to designing hoax verification foundation along with better security techniques, would become crucial and pivotal in the years to come.

G. Security Technology Integration

Implementation of security in parallel with website development in large organizations is a much better solution. Microsoft's Security Development Life cycle (SDL), OWASP's Comprehensive, Lightweight Application Security Process (CLASP) and McGraw' Touchpoints [9] should be considered according to the size of the organization to integrate security with Technology. Preventing frauds from occurring at an early stage would be a lot beneficial in upcoming years.

H. Artificial intelligence

As Artificial Intelligence and machine learning [10] takes pace, and begins to affect an ever increasing number of ventures, it's assumed to play a key role in cybersecurity. Because the fight with cyber espionages and cyber hackivists moves so rapidly, machine-learning models that can anticipate and precisely distinguish threats quickly could be a genuine shelter for Cyber Security experts. These models should be prepared and trained to fight with the cyber criminals.

IV. DOMAINS OF CYBER SECURITY

There are copious domains of cyber security that are totally in context to protect devices from different sorts of malwares, data breaches, ruptures, assaults, and so forth. Fig. 3 shows the relationship between cyber security and other security domains. Researchers have classified these cyber security domains into five categories:-

A. Data Security

Data Security is the foremost significant kind of the information security. It is depicted as securing sensitive or critical data and information from a variety of risks through diverse safety measures, like, steganography, hashing, cryptography, compression, etc. This information can either stay in at least one stand-alone device or in fringe gadgets like hard drives, SD cards, Pen drives, and so forth. Such information is called 'information stored at rest'. The information can even be transmitted between at least two nodes or devices known as 'information in movement'. It mostly preserves confidentiality, integrity and availability of information. A ton of research has happened to safeguard data from data leakage and data theft.

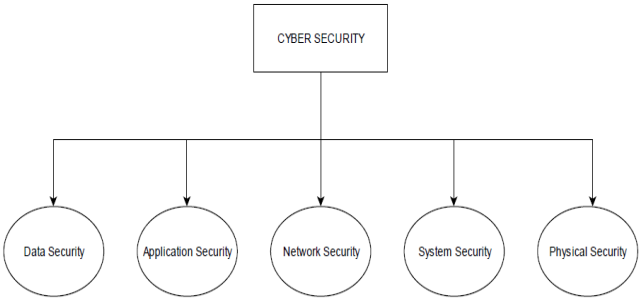

Fig. 3 Domains of Cyber Security

B. Application Security

Application security is the field of cyber security that considers enhancing the security of an application at the development stage itself. It involves usage of secure coding while programming to keep the application safe from different threats and vulnerabilities. These incorporate data breaches, digital assaults like those present in Open Web Application Security Project (OWASP) Top 10 vulnerabilities such as injection, cross Site Scripting, sensitive data exposure, security misconfiguration and so forth. Secure Development Lifecycle is supposed to be followed to safeguard the product from being damaged by malignant consumers.

C. Network Security

Network security is the precautionary measures taken by an organization to prevent unauthorized access

to network's private data, its users, or their devices. Firewalls, Intrusion Detection and Prevention System (IDPS), etc. are implemented to prevent unauthorized access and risks.

D. System Security

System Security involves controlling authentication and authorization to system assets that contain delicate information. The system should accordingly incorporate specific measures for protecting such information, and should thus control access to those parts of the system that contain sensitive information.

E. Physical Security

Protection of personnel, hardware, programming, devices and data from physical doings and events that could make real damage an individual, group or associations is termed as Physical security. This consolidates security from hardware or software failures, disastrous occasions, theft, thievery and vandalism.

V. COMPARATIVE STUDY OF DEFENSE APPROACHES IN CURRENT SCENARIO

Security issues weaken the prolonged growth, modernization, and adoption of technology. Several researchers in various domains of cyber security have carried out a lot of work.

In paper [11], the issue of recognizing and organizing defender framework vulnerabilities utilizing statistical and machine learning to investigate an expansive amount of information (e.g., digital, web based life) on lately identified framework vulnerabilities to "learn" classifiers that foresee the probability and time, when new vulnerabilities might be misused, has been discussed. This ensures computer systems against interruptions and various vindictive practices proactively through inferring two new methodologies intended for safeguarding system: 1.) a bipartite outline based exchange learning computation which enables information relating to past strikes to be exchanged for application against novel attacks, consequently increasing the rate with which secure systems can viably respond to a new attack, and 2.) a manufactured information learning procedure that encounters vital danger data to convey snare information for use in learning real secure activities, happening as expected in genius protections that are astounding against both present and (close) future assaults. Again an efficient approach is required to secure computer networks proactively which is missing in this study.

The study [12] reveals the innovation and proportions of information security in remote frameworks from the point of view of responsive and volatile security methods. Apart from this, it also exposes the passive methods utilized to enhance information security. Passive approach again secures data only after an attack or data breach has occurred.

In paper [13], implications of Big data, Artificial Intelligence (AI) and AI for information security have been discussed and the ICO's points of view on these have been explained. In addition, the examination of big data using methodology made possible by AI has made proposals for information security. This paper reviews about what all can be done to secure data with next generation technologies as the present techniques will not be enough anymore.

The work [14] recognizes present and potential automated risks to robotics at the hardware, firmware/OS, and application levels. Attack circumstances are shown and inspected at each level. Additionally, the financial and human security impact of an electronic attack on robots is investigated. Finally, possible countermeasures are proposed. The use of advanced attacks on robots is discussed and this paper moreover portrayed the impact of a digital assault on human security for military, transportation, and so forth. Security issues at system level are discussed that again demonstrate the need of proactiveness in implementing security.

In paper [15], the security and defense challenges in the health division have been outlined. The fundamental focus has been on the most recent proposed procedures in context of anonymization and encryption, and the future research in this area has also been examined. The security preservation policies that have been used until now as medical assistances are assessed and analyzed for encryption and anonymization procedures. Reactive approach again seems to be inefficient in the Health sector because of novel issues arising with the advent in technology.

The study [16] presents the data security measurements and the examination of data compression techniques. The parameters that have been considered are speed, applications, compression ratio and focal points. Association of different data compression methods are looked into in this paper for guaranteeing information security. Speculations on reactive, proactive and preventive Data security strategies have also been given.

In framework [17], called Reactive Redundancy for Data Destruction (R2D2) Protection, buffers are written before they can achieve a capacity situation, chooses whether the capacity is damaging, and block the data in obliteration. They mediate the inspection in the Virtual Machine Monitor (VMM) through a framework known as Virtual Machine Introspection (VMI). This has the favorable position that it does not rely upon the entire OS as a foundation of trust, in contrast to prior structures that protected Crypto Ransomware, due to the unit of the examination and checking inside a VMM. This study basically gives an idea how ransomware can be prohibited by reactive data redundancy approach. A proactive approach can be a better option.

The study [18] presents the progress in the arena of employing artificial intelligence strategies aimed at fighting digital violations, in order to show that in what way these techniques can be effective in finding and envisioning wrongdoings digitally, and additionally provide the augmentation for future work. Artificial intelligence techniques are now being used to help individuals in combating advanced bad behaviors, as they provide

both flexibility and learning abilities to IDPS software.

In the paper [19], another methodology for passive information security is perceived in a virtualized PC condition in perspective of unimportant intruding powerful sensors sent vertically transversely over virtualization layers and on a level plane inside a virtual machine instance.

The sensor streams are separated using an association of CEP engines and questionnaire to help the execution, and the results of the examination are used to trigger actions in light of recognized security malfunctions. They even use a novel event store that supports speedy event logging for separate examination of accumulated recorded data. Investigations have demonstrated that the proposed framework can achieve an immense number of perplexing and stateful recognition manages at the same time with elite and low dormancy.

The work [20] investigates security in Process Aware Information Systems (PAIS) and goes for constructing a regular understanding of wording in this remarkable circumstance. Besides, it inquires about which security controls are currently associated in PAIS. Twelve recognized security guidelines are given in the vicinity of security notions, agreement and privilege escalation, and so forth. This paper only focuses on authentication and authorization regulations that are reactive in nature but the systems can be more secure if we consider other factors of system as well, proactively.

In a different paper [21], a three-layer model is proposed for evaluating the proficiency of numerous Moving Target Defenses. This model is arranged as an undertaking to fill the gap among existing evaluation procedures and capacities as a structure for Moving Target Defense relationship. This model fills space between low-level and complex techniques. Yet again this Reactive Model only surveys security methodologies.

In the work [22], a methodology named Genetic Algorithm (GA) and Artificial Immune System (AIS) (GAAIS) is proposed, for dynamic intrusion recognition in AODV-based MANETs. The execution of GAAIS is evaluated for recognizing a couple of sorts of directing attacks reenacted using the NS2 test framework, for instance, Flooding, Blackhole, Neighbor, Surging, and Wormhole. GAAIS can acclimate to real-time framework topology changes utilizing two refreshing strategies: fractional and over-all. Machine Learning Techniques can be applied proactively to raise security in MANETs.

A survey [23] is shown on available data security techniques, focusing on specific uncertainties as well as necessities pertaining to their use in data warehousing circumstances. It also points out challenges and open entryways aimed at forthcoming exploration in this area. In this work, until now available data security answers for data warehousing, discussing their issues and impact in DW execution and versatility essentials, have been shown.

This work [24] discussed Reactive Policy Creation in which customers can refresh their arrangements dynamically in light of access requests that would not for the most part succeed. Receptive approach creation stand better in contrast with static access controls.

To help the amalgamation of security ahead of plan in the SDLC phases, another paper [25] examined approach for assessing security in the midst of the planned phase by neural method. Their disclosures show that by means of setting up a back propagation neural method to perceive attack structures, plausible harms can be recognized from framework displayed to it.

Because of Systematic Literature Review, a resultant practical procedure which can bolster the execution of an active criminology framework is anticipated in this work [26]. Combination of proactive and reactive investigation method is proposed that can both continuously learn and automate the process.

An arrangement of compromised strategies is explored in this study [27], to build information fine-tuning and self-learning mechanisms in an extensive variety of security frameworks. The anticipated self-learning strategies are amalgamated with other web/information extraction, abnormality location, factual techniques, and show new approaches in the advancement of mutual transformative frameworks.

In the study [28], a scheduler for Secure Multi-Execution (SME), is proposed, which makes it conceivable to safeguard the request of productivity. Employing SME, an innovative new amalgamation among examining and SME, called multi-execution monitor, which raises cautions just for activities breaching the non-obstruction thought of ID-security for receptive frameworks has been introduced. This strategy precisely perceives actions that reveal information under the idea of ID-security.

In the paper [29], welfare and security are chosen as two criteria of consistency for Real Time Reactive System and a formal method to manage building a dependable structure is proposed. The advancement procedure relies upon segment innovation. By using Component based development it is possible to officially decide reliable fragments and create them. This methodology drives us to a procedure for the affirmation of trust using model checking, which has given the impression of being a promising strategy for the affirmation of security properties for RTRS.

The work [30] introduced another methodology ‘Active Security’ for executing security frameworks, having the capacity to consequently react to newborn security threats. The idea of convergence of this work is fusing a security foundation where intrusion detection frameworks, vulnerability scanners, firewalls and other security devices can impart and react to changing security perils. The Active Security approach shields the clients from malevolent action by progressively filtering the system, constantly checking it to stop any further bad behavior.

The paper [31] tries to clarify the Big Data security and protection challenges. It tells about various challenges like access control, encryption, compliance, data leakage, etc. to be dealt with much better security.

The work [32] thinks about the essential thoughts and analyzes the fundamentals of information security issues associated with Cloud. Subsequently they magnify each issue discussing their inclination and existing plans, if available. Distinctive attention is given to privacy, integrity and accessibility of information to audit, and execute the controls and compliances keeping in mind information security and defense. In the course of their research, they considered dangers like insiders and verified the general application circumstances just as mission-basic ones so as to keep up CIA of information.

Table I Comparative Analysis of current security mechanisms in various domains of Cyber Security

Security Domain	Work Done	Security Approach (Reactive /Proactive)	Research Gaps
Network Security [11]	Statistical and machine learning approaches have been considered to analyze a broad range of data (e.g., cyber, social media).	Proactive	Ultimate fate of proactive protection method to deal with further dangers, which include existence of invader and protector along with the enhancement of new proactive defense is by suitably joining information investigation strategies (e.g., AI) with social models.
System Security [14]	This research discriminates current and possible digital threats to robotics at the device, firmware/OS, and application levels.	Reactive	Just the current risks are considered even when the future is advancing towards Artificial Intelligence.
Data Security [16]	Data security techniques and the examination of data compression methods have been carried out.	Reactive, Proactive	Data hiding and data encryption techniques have been discussed for securing data proactively but still these strategies are inadequate if the attacker steals the password of the genuine user.
System Security[17]	The approach used in this work is Reactive Redundancy for Data Destruction (R2D2) Protection. In this, the examination is intervened in the Virtual Machine Monitor (VMM) through a system known as Virtual Machine Introspection (VMI).	Reactive	The approach involves a lot of overhead, thereby does not provide enhanced system security.
Network Security [18]	Advancement made so far in the field of applying AI techniques for battling computerized infringement, to indicate how these strategies can be effective for disclosure and expectation of computerized wrongdoings, and also to give the expansion for future work.	Reactive	Unsupervised machine learning algorithms can be contemplated to create Intrusion Detection and Prevention Systems (IDPS), to deal with real time attacks.
System Security[19]	Another approach for reactive security is observed in a virtualized PC condition in view of negligibly meddling dynamic sensors sent vertically crosswise over virtualization layers and on a level plane inside a virtual machine instance.	Reactive	The paper has exhibited that the framework can be utilized for responsive security observing regarding execution, yet, not how it ought to be utilized. Consequently, determining fitting sensors, CEP questions and activities for a few kinds of potential assaults is a testing undertaking for future research.

System Security [20]	This paper explores security in Process Aware Information Systems.	Reactive	Study shows that security in PAIS is a challenging interdisciplinary research field that assembles research methods and principles from security and PAIS but still many open challenges remain.
System Security[21]	A three-layer model is proposed to survey the adequacy of various Moving Target Defenses.	Reactive	An increasingly intensive approach is required, to expand vulnerability and clear multifaceted nature for attackers.
Network Security[22]	Genetic Algorithm (GA) and Artificial Immune System (AIS), called GAAIS, for dynamic interruption identification in AODV-based MANETs.	Proactive	Hybrid methodology would be better to detect invasions in MANET's having dynamic topology.
Physical Security[24]	Policy Creation has been done. In this, the customers can restore their strategies with time in light of access requirements.	Reactive	Access Controls, to store and share progressively digital at home, just change after some issue emerges yet does not change consequently by consistent learning.
Application Security[25]	Neural System approach is discussed in SDLC.	Reactive	To moreover upgrade the execution of the neural framework system as a gadget for reviewing security in software design diagrams, a structure is required for suggesting plans that can keep the recognized attacks.
Application Security[26]	Multi-component procedure for reactive and proactive methodologies for digital forensic exploration.	Both Reactive and proactive	Two noteworthy issues have been left out: 1) the capacity to foresee an occasion (an assault) proactively, and 2) enhancing the proactive segment by giving a criticism circle at whatever point the proactive or the responsive segment is finished up.
Application Security[27]	Self-learning strategies are consolidated with web/information mining, abnormalities identification and statistical methods.	Reactive	Dynamic web environments have not been taken into consideration.
Network Security[30]	Active Security approach is applied, in which the network is scanned dynamically in order to cease any further illegal behavior.	Reactive	Data breach is yet conceivable in light of the fact that no proactive checking of information is being done.
Data Security[31]	Big Data security and protection challenges like access control, encryption, compliance, data leakage, etc. are discussed.	Reactive	No data security at real time is considered.

VI. CRITICAL ANALYSIS OF SECURITY MEASURES

Critical challenges are increasing in the "Cyber Space Domain". Prediction and prevention of attacks at real-time is missing in the existing approaches. The current approaches in various security domains are mostly reactive in nature. The prevailing techniques concentrate primarily on the existing defense mechanisms. The upcoming attack technology would overtake the existing defense procedures. The security operations applied on application security, network security, data security, system security have been mostly detective and preventive in nature. The researchers have not considered the best practices by doing Risk Analysis to implement security at application, network, data and system levels. Mitigation techniques like supervised Learning, cryptographic measures, patches at operating system level, and so on have been considered for employing security in enterprises, which wait for the attacks to occur and then later identify the reason of their occurrence to prevent the attacks from striking in future.

VII. CONCLUSION

Identifying and mitigating a security issue and also pattern analysis of attacks are hardly taken into consideration. There are a number of ambiguities present in the contemporary systems and a lot needs to be done to enable 360^{o} protection for proper security. As enumerated in the above papers there are large gaps which needs proper research and integration. With the availability of higher processing power

coming at a very cheap rate as well as the progress made in the field of Artificial Intelligence, a novel approach of proactive protection as well as real-time analysis of intrusion pattern could be formulated and implemented easily. Another thing which could lead to better security handling, is the inculcation of security aspects at the designing phase of any architecture of systems, applications or networks. The best approach for security is to be prepared for the worst conceivable scenario and plan for any failure in the future.

ACKNOWLEDGMENT

We are grateful to Dr. Kingshuk Srivastava, Assistant Professor (SG), School of Computer Science (SCS), University of Petroleum and Energy Studies (UPES), Dehradun for his assistance in writing this paper. We also wish to express our gratitude towards Dr. Neelu Jyoti Ahuja, Head of Department, SCS, UPES, Dehradun and Dr. Manish Prateek, Dean, SCS, UPES, Dehradun for their unconditional support during the course of this research.

REFERENCES

1. "Industrial Revolution 3.0 | HuffPost." [Online]. Available: https://www.huffingtonpost.com/ignacio-peaa/industrial-revolution-30_b_5806874.html. [Accessed: 15-Oct-2018].
2. "Gen-V Cyber Security | Check Point Software." [Online]. Available: https://www.checkpoint.com/gen-v-cyber-security/. [Accessed: 15-Oct-2018].
3. "Boost Business Prospects In Cyber Security Market | MarketsandMarkets Blog." [Online]. Available: http://www.marketsandmarketsblog.com/cyber-security-market.html. [Accessed: 13-Oct-2018].
4. "What is the Importance of Cyber Security in 2018 [14 Factors to Consider]." [Online]. Available: https://www.testbytes.net/blog/cyber-security-in-2018/. [Accessed: 13-Oct-2018].
5. R. Toshniwal, K. G. Dastidar, and A. Nath, "Big Data Security Issues and Challenges," International Journal of Innovative Research in Advanced Engineering (IJIRAE) vol. 42, no. 42, pp. 21–25, 2015.
6. N. vurukonda and B. Rao, "A Study on Data Storage Security Issues in Cloud Computing", Procedia Computer Science, vol. 92, pp. 128-135, 2016. Available: 10.1016/j.procs.2016.07.335.
7. Muthuswamy, Sujithra & Ganapathi, Padmavathi, "IOT Security Challenges and Issues – An Overview," UGC Sponsored Two Day National Conference on Internet of Things, February, 2016.
8. Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," Proc. - 2017 IEEE 6th Int. Congr. Big Data, BigData Congr. 2017, no. June, pp. 557–564, 2017.
9. B. De Win, R. Scandariato, K. Buyens, J. Grégoire, and W. Joosen, "On the secure software development process: CLASP, SDL and Touchpoints compared," Inf. Softw. Technol., vol. 51, no. 7, pp. 1152–1171, 2009.
10. Cncs.gov.pt, 2019. [Online]. Available: https://www.cncs.gov.pt/content/files/cybersecurity_and_the_role_of_artificial_intelligence-_arlindo_oliveira.pdf/.
11. R. Colbaugh and K. Glass, "Proactive defense for evolving cyber threats," Proc. 2011 IEEE Int. Conf. Intell. Secur. Informatics, ISI 2011, no. November, pp. 125–130, 2011.
12. A. Sari and M. Karay, "Reactive Data Security Approach and Review of Data Security Techniques in Wireless Networks," Int. J. Communications, Network and System Sciences, 2015, 8, 567-577.
13. S. Cetin, "Big Data, Artificial Intelligence, Machine Learning and Data Protection - Hukuk & Robotik", Hukuk & Robotik, 2019. [Online]. Available: https://robotic.legal/en/big-data-artificial-intelligence-machine-learning-and-data-protection/. [Accessed: 22- Jul- 2019].
14. D. W. Dorsey, J. Martin, D. J. Howard, and M. D. Coovert, "Cybersecurity issues in selection," Handb. Empl. Sel. Second Ed., pp. 913–929, 2017.
15. K. Abouelmehdi, A. Beni-Hessane, and H. Khaloufi, "Big healthcare data: preserving security and privacy," J. Big Data, vol. 5, no. 1, pp. 1–18, 2018.
16. J. Kurmi, "A Reassessment on Security Tactics of Data Warehouse and Comparison of Compression Algorithms," vol. 10, no. 5, pp. 847–854, 2017.
17. C. N. Gutierrez, E. H. Spafford, S. Bagchi, and T. Yurek, "Reactive redundancy for data destruction protection (R2D2)," Comput. Secur., vol. 74, pp. 184–201, 2018.
18. S. Dilek, H. Cakır, and M. Aydın, "Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review," Int. J. Artif. Intell. Appl., vol. 6, no. 1, pp. 21–39, 2015.
19. L. Baumgärtner, C. Strack, B. Hoßbach, M. Seidemann, B. Seeger, and B. Freisleben, "Complex event processing for reactive security monitoring in virtualized computer systems," Proc. 9th ACM Int. Conf. Distrib. Event-Based Syst. - DEBS '15, pp. 22–33, 2015.
20. M. Leitner and S. Rinderle-Ma, "A systematic review on security in Process-Aware Information Systems - Constitution, challenges, and future directions," Inf. Softw. Technol., vol. 56, no. 3, pp. 273–293, 2014.
21. J. Xu, P. Guo, M. Zhao, R. F. Erbacher, M. Zhu, and P. Liu, "Comparing Different Moving Target Defense Techniques," Proc. First ACM Work. Mov. Target Def. - MTD '14, pp. 97–107, 2014.
22. F. Barani, "A hybrid approach for dynamic intrusion detection in ad hoc networks using genetic algorithm and artificial immune system," 2014 Iran. Conf. Intell. Syst., pp. 1–6, 2014.
23. R. J. Santos, J. Bernardino, and M. Vieira, "A survey on data security in data warehousing: Issues, challenges and opportunities," EUROCON 2011 - Int. Conf. Comput. as a Tool - Jt. with Conftele 2011, pp. 5–8, 2011.
24. M. L. Mazurek, P. F. Klemperer, R. Shay, H. Takabi, L. Bauer, and L. F. Cranor, "Exploring reactive access control," Proc. 2011 Annu. Conf. Hum. factors Comput. Syst. - CHI '11, p. 2085, 2011.
25. A. Adebiyi, J. Arreymbi, and C. Imafidon, "Security Assessment of Software Design using Neural Network," Int. J. Adv. Res. Artif. Intell., vol. 1, no. 4, pp. 1–7, 2012.
26. S. S. Alharbi, J. Weber-Jahnke, and I. Traore, "The Proactive and Reactive Digital Forensics Investigation Process: A Systematic Literature Review," Int. J. …, vol. 5, no. 4, pp. 87–100, 2011.
27. V. S. Jotsov, "Machine self-learning applications in security systems," Proc. 6th IEEE Int. Conf. Intell. Data Acquis. Adv. Comput. Syst. Technol. Appl. IDAACS'2011, vol. 2, no. September, pp. 727–732, 2011.
28. D. Zanarini, M. Jaskelioff, and A. Russo, "Precise enforcement of confidentiality for reactive systems," Proc. Comput. Secur. Found. Work., pp. 18–32, 2013.
29. V. Alagar and M. Mohammad, "A Component Model for Trustworthy Real-Time Reactive Systems Development," Electron. Notes Theor. Comput. Sci., pp. 1–15, 2007.
30. G. Eschelbeck, "Active Security - A proactive approach for computer security systems," J. Netw. Comput. Appl., vol. 23, no. 2, pp. 109–130, 2000.
31. K. Choksi, N. Dalal, K. Gupte, and A. Jivani, "Security and privacy challenges in big data", International Journal of latest trends in Engineering and Technology, vol. 7, no. 3, pp. 313–318, 2016.
32. S. Yu, W. Lou, and K. Ren, "Chapter 5 . 3 : Data Security in Cloud Computing," Univ. Arkansas, pp. 1–29.

AUTHORS PROFILE

Tripti Misra is pursuing Ph.D in Computer Science and Engineering from University of Petroleum and Energy Studies, Dehradun. She is an M. Tech in Software Engineering from MNNIT Allahabad. She has total 7 years of experience in academia and industry. She is currently working as an Assistant Professor (Senior Scale) in the Department of Systemics, School of Computer Science, UPES Dehradun. Previously she was working as Project Engineer I in CDAC Hyderabad in association with Sardar Vallabhbhai Patel National Police Academy, Hyderabad, on National Digital Crime Resource & Training Center (NDCRTC) Project. There she was Involved in training of Law Enforcement Personnel from Police, Revenue and Judiciary in domain of Cyber Forensics. Her area of interest is Information Security, Machine Learning and Computer Networks.

Dr. Kingshuk Srivastava is working as a faculty for the last eight years in UPES as a faculty in the "School of Computer Science", after a short stint in the industry with "Planman Technology". He has obtained the degree of B.Sc.-Physics & M.Sc.-Physics (Electronics) from LNMU. Dharbhanga. He was the topper and Silver Medallist in M.Tech from UPES. He also earned his Ph.D in Computer Science Engineering from UPES. His field of research has

been in AI, Data Warehousing, Data Science and NOSQL databases. He has conducted workshops on Big Data Hadoop, AI and Machine Learning under Management Development Program. He has supervised and mentored Three PhD & several projects under Business Analytics, Business Intelligence and Big Data IoT. His area of interest consists of Big Data, Business Analytics, Business Intelligence, Storage Technology, Oil & Gas sector and Data Warehousing.

Prof. Rajeshwari has around 16 plus years of expertise in the areas of IT services and operations, IT infrastructure management, Education, Training, Curriculum design & development, project management, ISO. She is interested in E-learning, Social Network, Mobility, Analytics, Cloud Solutions for Education Industry and Digital Marketing. She is presently working as Assistant Director –Products (Academic Programs).