*International Journal on Emerging Technologies* **11**(2): 939-947(2020)

**ISSN No. (Print): 0975-8364**
**ISSN No. (Online): 2249-3255**

# Study of Latest Cybersecurity Threats to IT/OT and their Impact on e-Governance in India

***Kishore K. Morya[1] and Mahesh Singh[2]***
*[1]Associate Professor, School of Management, G.D. Goenka, University, Gurugram (Haryana), India.*
*[2]Ph.D. Scholar, School of Management, G.D. Goenka, University, Gurugram (Haryana), India.*

*(Corresponding author: Mahesh Singh)*

*(Received 25 January 2020, Revised 17 March 2020, Accepted 20 March 2020)*
*(Published by Research Trend, Website: www.researchtrend.net)*

**ABSTRACT: Being progressively interconnected world today, the information security system must be set up to counter emerging vulnerabilities that may occur as a result of technological advancement. In the complex and dynamic arena of internet, the challenges inherent in safeguarding Information infrastructure is drastically increasing, possibly as a factor of the ubiquitous existence of services etc. depending on these networks. These networks are exposed to cyber-attacks due to various flaws in the system. Therefore, it is essential to accelerate on the security that covers the application software and infrastructure to give the governance an effective internet without any possible risk of being rigged.**

**The study discusses about the cyber security issues in today's era as technology is touching every sphere of life so as e-Governance applications. Study also focuses on how e-Governance is made more secure and what type of safety features to be adopted, have to be safe, secure and reliable atmosphere by various technologies in e-Governance functions i.e. cloud computing, e-commerce, social networking, online government banking system, payment of online bills and also outline here in what way to decrease the online offenses by strengthening the safety aspects of e-Governance systems. However, during study it is felt that limited studies have been done on cybersecurity of IT/OT infrastructure used for e-Governance in India.**

**Keywords:** Cybercrime, Cybersecurity, Cyber Threats, e-Governance, IT/OT, Industrial Control Systems, Information Communication Technology, Security Breaches.

**Abbreviations:** ICS: Industrial Control Systems, ICT: Information Communication Technology, IT/OT: Information Technology/Operational Technology, SCADA: Supervisory, Control and Data Acquisition.

## I. INTRODUCTION

The increasing digitization of organisations and the associated networking of almost all regions are generating remarkable commercial potential. At the same time the improved networking is giving upsurge to new threats that need a quick and rigorous reaction. The constant increase in the figure of cyber-attacks [1] in recent years has urged policymakers to make conforming procedures and protocols for cybersecurity. The aim of these requirements is to safeguard critical infrastructures in order to guarantee continuous services to citizens and strength to the country. Cybersecurity implies to the capability of controlled access to network, systems and the data they have. Digital infrastructure is considered a reliable and trustable cyberspace where cybersecurity measures are effective. The scope of cybersecurity covers the security of IT systems within the organisation, the digital systems upon which they rely including critical infrastructures and cyberspace. Cybersecurity impacts the development of Information Technology and Internet services to a great extent. It is essential to improve cybersecurity to have protected critical information infrastructure for country's security and commercial viability [2]. Dependency on Information Technology of the public has increased in all areas of human activities such as e-commerce, finance, health care, energy, entertainment, media, and national security [1]. Latest research reveals that the aspirations of public towards personal information and confidentiality have gone up since 2006 [3].The study will provide inside about challenges and measures related to cybersecurity of e-Governance applications.

**Objectives:**

– To study cyber threat's incidents and trends related to IT/OT.

– To analyse the issues, challenges and impact of cyber threats on e-governance in India.

– To illume on cybersecurity measures in e-governance.

## II. LITERATURE REVIEW

### *A. Global Impact of cybercrime*

Information security trade is on high alarm due to various new and growing cybersecurity threats. Data and resources of organisations, individuals and governments are at continuous threat due to increasingly refined cyber-attacks including spyware, phishing, artificial intelligence and machine learning, cryptocurrency and more. As per University of Moore [4], the sector remains in suffering from acute scarcity of cybersecurity experts and professionals caution about the risks which are more sophisticated than ever because the cybercrime rampant even threats tremoring civic trust in such precious ethics as individual secrecy, democracy and capitalism.

It is true that most of the globe not equipped well to tackle Cybercrime. It is unpredictable, often unnoticeable and has clear scope due to which a hacker in one part of the world can enter into a system at other corner easily which can create boundaries problems to tackle. Consultancy India reported on its website on June 4 2018 [5], India positions relatively high on the universal list level of cybercrime as well. By the proportion of criminallycontrolled schemes as a measure, the United States is at the top being worst affected by cybercrime with 23%, then China with 9%. Spain, Brazil, Britain and Germany fall between 4% and 6% with respect to percentage of effect of cybercrime. Though, India registers 3% of unethically penetrated systems but stands third by the total figure of affected systems.

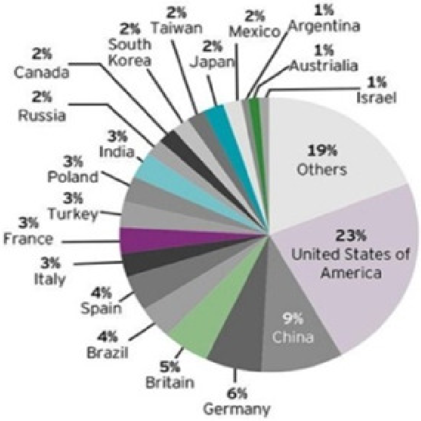

**Fig. 1.** Global Impact of cybercrime [5].

*B. Cybersecurity incidents and cybercrime over the years*

Cyber threats becoming more refined and capable, the influence of cybercrime is accumulative, and the attacks are also increasing in volume and variety as well. "India was the third worst affected by WannaCry (an advanced ransomware attack) among more than 100 countries those were hit" [6].

As per Indian Computer Emergency Response Team [7], the number of cases reported in year 2018 increased exponentially compared to during the years2014-2017 and cybercrime cases registered during the years 2014-2016 gradually increased whereas during the year 2017-2018 this increase is sharp as per the data kept by National Crime Record Bureau [8].

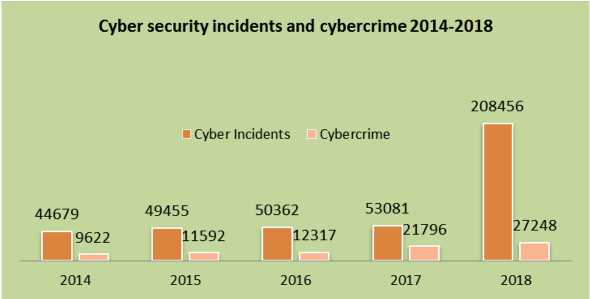

**Fig. 2.** Cybersecurity incidents and cybercrime.

*C. Biggest Data Breaches based on Public Affected*

Data is increasingly becoming one of the most precious resources in the recent ecosphere. The digital giants that dominate data are possibly the most influential establishments in the world, encouraging current talks about anti-trust regulation and digital secrecy. In spite of the exceptional value organized by these units, still companies such as Facebook are exposed to the derivative of the fast change to digitization - the data breach epidemic. Every data breaches had an effect on millions of individuals, and offer diverse instances of how an entity can be compromised or leave an unusual number of records exposed. Infographic is as per Fig. 3. Few of data breaches as per UP Guard [9] given below:

– Yahoo - 3 billion, October 2017
– Aadhaar - 1.1 billion, March 2018
– First American Financial Corp., 885 million, May 2019
– Verifications.io - 763 million, February 2019
– Yahoo - 500 million, 2014

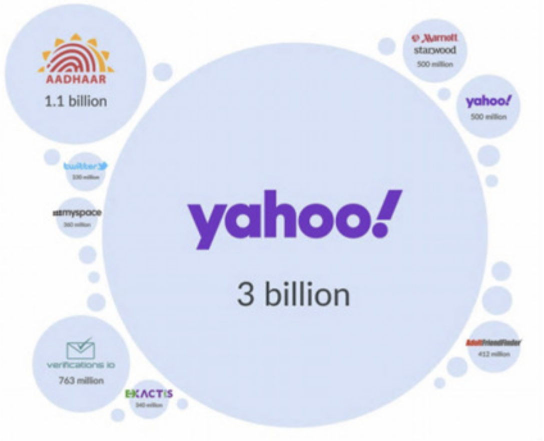

**Fig. 3.** Biggest data breaches infographic [9].

*D. Research Gaps*

Based on review of various literature from 2011 to 2018, we have established subsequent descriptions as major research gaps in the cybersecurity of e-Governance while using critical infrastructure in Indian environment:

– Restructuring of policy and procedures is required for confidentiality and security during interoperability for successful e-Governance. Cybersecurity framework will ensure safe exchange of data of e-Governance [10].

– There is scope of further research to address security of data and information infrastructure at appropriate levels in the e-Governance. Requirement of specific architecture of systems to meet objectives of e-Governance vision and policies to adopt modern technologies [11].

– There are obstacles like digital disparity between urban and rural, knowledge, poverty, safety and execution cost of e-Governance initiatives [12].

– It is clear that a lot of scope is available for further research in the area of information security of e-Governance in India. Also scope is there to develop exhaustive and functional cybersecurity model [13].

– Security is critical for successful implementation of e-Governance initiatives. Study also shows that there are pretty incidences when decision-makers deferred the implementation of hi-tech infrastructure due to high cost of execution and operation [14].

### *E. Recent Security Breaches worldwide*

Some of the quarters have been advocated that the anxiety over cybersecurity gaps is exaggerated [15, 16]. In August 2011, the ease of penetration of ICS infrastructure was established at a Black Hat conference gave emphasis to the safety of numerous ICS systems [17]. To highlight the gravity and incidence of ICS security, a few latest cases reported in the community province by news media are enumerated here:

“**Electricity Grid in U.S. Penetrated By Spies ", April 2009:** Cyber spies breached the electric grid of U.S. and dumped software means which can be utilized to harm or interrupt the grid. State Security experts specify that espionages originated from Russia, China, and different nations too. The difficulty in identifying identity in cyberspace inhibits exact information of who is accountable or what their intensions are, but electronic imprints of pilferage information have established links to Russia and China. "Over the past several years, we have seen cyber-attacks against critical infrastructures abroad, and many of our own infrastructures are as vulnerable as their foreign counterparts," U.S. National Intelligence, Director, Dennis Blair informed legislators. "A number of nations, including Russia and China, can disrupt elements of the U.S. information infrastructure" [18].

**“Siemens: Stuxnet worm hit industrial systems ", September 2010:** According to Siemens, “a sophisticated worm designed to steal industrial secrets and disrupt operations has infected at least 14 plants." It is believed that Stuxnet is aimed for nuclear augmentation installations of Iran. Though Stuxnet creator is unverified, 60% of stated bugs were within Iran. Spreading of worm was done using an earlier unidentified MS Windows weakness, usually from pen drives. Default passwords were used by intruder while attacking Siemens ICS [19].

**"Conficker infected critical hospital equipment", April 2009:** "The Conficker worm infected several hundred machines including critical medical equipment in an undisclosed number of U.S. hospitals."[20]It is established that infested Windows computers were used to spread Conficker, yet it is to be known in what way the control setups like MRI machines and heart monitors were infested.

**“Computer Virus Hits U.S. Drone Fleet", October 2011:** "A computer virus has infected the cockpits of America's Predator and Reaper drones, logging pilots' every keystroke as they remotely fly missions over Afghanistan and other warzones" [21]. It is unidentified where this newest virus invented or its anticipated utility. Other safety defects of the drone systems were already known to have been misused by aggressive revelries, for example video transmissions do not encrypted by many drones.

**"Attack Code for SCADA Vulnerabilities Released Online", March 2011:** Luigi Auriemma, security scholar in March 2011 sent SCADA intrusion code to a security emailing recipients. Seven susceptibilities were used in SCADA environment which are normally employed in oil and natural gas installations, water treatment setups, and plants. Amongst the 34 exploits released, effective victimization of denial-of-service assaults, buffer-overflow susceptibilities, foreign file injection into machines, enablement of remote execution for malicious code and altered data displayed to operators monitoring system operations during demonstration of tests. The scholar specified that he did not know much about the SCADA systems before beginning his tests with software and documentation easily obtainable by anyone, emphasizing SCADA security weaknesses [22].

**“Researchers warn of SCADA equipment discoverable via Google", 2011:** Demonstration during a Black Hat conference using a Google search engine found the address of a RTU monitoring a pump station [17]. Search engines used to identify and directly access controllers and standard software programs are freely available, such as ERIPP, SHODAN, and Google. Security exploits can be designed fairly quickly due to readily availability of documentation of common ICS codes [23].

**“90% of Infrastructure Security Pros Have Been Hacked in the Last Two Years”, April 2019**

As per the study of Cybersecurity Company, Tenable Inc. [24], “Cybersecurity in Operational Technology: 7 Insights You Need to Know”, the results identify the extent of cyber-attacks experienced by critical infrastructure operators and professionals in businesses using ICS. Report revealed that ninety percent tICS environments had damaged over the past two years by at least one cyber-attack and 62% experienced two or more attacks.

### *F. Few Emerging Security Threats to IT/OT*

Recent technology and society’s continuous association to the Internet permits additional creativeness in corporate than ever before including the gray market. Cyber offenders are judiciously realizing novel techniques to tap the critical networks in the world. Safeguarding industry data is an emergent task but alertness is the first phase. Here are the few emerging threats to information security [25].

**(a) Convergence of IT and OT:** Integration of modern ICS with corporate LAN for remote monitoring and control and allowing remote access of ICS to vendors and support personnel, these rights of access to ICS invite many openings to breach security such as:

– **Denial of Service (DoS) attacks**-Invalidated sources and inadequate access rights permit attackers in harming OT systems to perform DoS attacks on vulnerable unpatched systems. ICS are open to usually known TCP/IP DoS attacks like SYN flooding, low-rate DoS (LDoS) attacks influencing TCP's retransmission time-out mechanisms, or buffer-overflow scenarios [26, 27].

– **Use of outdated and open source protocols**-ICS operations normally use outdated, insecure protocols such as FTP and Telnet. Modbus/TCP, Ethernet/IP and DNP3 SCADA communication protocols of ICS for control devices normally do not need any validation to remotely execute commands on a control device, and no encryption replacements available [28, 29].

– **Absence of Basic access control implementation**-Most devices need most basic access control isolating framework software mode versus application program mode. Server and terminal authentication is either not exist or entirely useless. Distinction of access rights among administrators and end users is usually absent or not employed [27].

– **Man-In-The-Middle Attacks**-Network intruders can influence in-transmission directions, commands, or alarms due to absence of encryption and mutual authentication of ICS. Reiteration attacks can activate automatic system reactions affecting in erratic malfunctions. Prompting system operators to take wrong and probably risky human intervention due to wrong monitoring data presented by spoofing bouts. Network sniffing may expose secret data to invisible seizure for governmental or industrial spying, radical attacks, or felonious chases [26, 28].

– **Corrupted Control System Device**-Control logic software is not secure and can be smoothly changed. Corrupted devices can end in system harm, disruption, or safety hazards. Firmware is not secure, making it possible to change configuration settings or push malicious code over Ethernet in many cases. Successive device failure or random functionality may result in DoS events [32, 33].

**(b) Technological Advancement with Weak Security:** Technological advancement is happening every day. Most likely, new devices have Internet access in some form or other but no strategy for security. This reveals a very severe threat – each unsafe connection means susceptibility. The fast growth of technology is evidence to researchers, yet safety lags critically [30].

**(c) Social Media Bouts:** Cyber offenders are utilizing social media as a platform to issue a multifarious geographic attack called "water holing". The attackers detect and taint a collection of websites they think participants of the intended organisation will access [31].

**(d) Mobile Malware:** Security specialists have perceived threat to mobile device safety since the initial phases of their access to the Internet. The nominal mobile filthy act amid the long list of latest occurrences has users far less worried than they would be. As our culture's strong dependence on mobile phones and how slight cyber offenders have targeted them, it generates a shattering hazard.

**(e) Access through Third-party:** Cybercriminals desire the route of least resistance. Goal is the poster boy of a key set-up attack through third-party entry points. The international retailer's HVAC dealer was the unlucky supplier whose IDs were whipped and used to snip commercial data records for 70 million clients [32].

**(f) Default Configuration:** Big data tools have the facility to be tailored to suit an organisation's requirements. Firms remain to disregard the significance of correct security configuration settings. The New York Times became target to a data breach as a consequence of applying only one of the few, critical functionalities desired to totally shield the organsation's information [33].

**(g) Obsolete Security Software:** Updating security software is an elementary technology management exercise and a required move to protect massive data. Program is developed to protect against identified risks. That implies that any new wicked code that knockouts an old form of security software will go unnoticed [34].

**(h) Social Engineering:** Cybercriminals know invasion skills have a shelf lifecycle. They have inclined to trusted non-technical means like social engineering, which depend on social dealings and emotional manipulation to get access to personal information. This method of invasion is random and effective [34].

**(i) Absence of Encryption:** Shielding sensitive commercial information in transfer and while storing is a requirement a small number of industries have yet to embrace, in spite of its usefulness. The health care sector tackles exceptionally complex information and realizes the severity of losing it – that is why HIPAA compliance needs each device to be encoded [34].

**(j) Business Data on Private Devices:** Whether a business gives company phones or not, business information is still being retrieved on personal devices. Mobile management techniques exist to curtail functionality but safeguarding the gaps has not made it to the important list for various establishments.

**(k) Insufficient Security Expertise** – Spending in software that observes the safety of a system has become a rising movement in the enterprise space after 2014's lapses of information breaches. The software is programmed to provide alarms when invasion efforts happen, yet the alarms are only valued if somebody is accessible to resolve them. Businesses are trusting too greatly on machinery to entirely defend against bout when it is intended to be a managed technology [34].

### *G. Future Risk Horizon*

During next few years, the very bases of today's digital domain will wobble – aggressively. Advanced and firm attackers, along with seismic variations to the way organisations manage their operations, will unite to expose even the robust set-ups. Only organisations with strong measures will stand tall. ISF report "Threat Horizon 2020" [35], presents nine threats that organisations across industries and counties can anticipate to face in near future.

(a) Virtual and physical attacks syndicate to smash industrial resilience Nation states and terrorists will associate traditional armed force with their increasingly refined cyber arsenals to launch hybrid bouts that generate maximum effect.

(b) Satellites create chaos on the earth Inactivating or hoaxing signals from GPS will place lives at danger and effect international tourism and finance markets. Attackers may also aim media, communications, climatological and armed functions to further interrupt operations and trade.

(c) We aponised tools make organisations defenceless Rivals targeting to inflict damage will take benefit of weaknesses in connected devices such as thermostats, dishwashers, kettles and refrigerators to create voltage surges strong enough to blow out regional power grids.

(d) Quantum weapons race weakens the digital economy those who develop or gain quantum computing technology will be capable to disrupt current encryption standards. With an essential safety mechanism rendered outdated, information and communications of all kinds will suddenly become susceptible.

(e) Artificially intelligent malware amplifies attackers' capabilities Attackers will take benefit of innovations in artificial intelligence (AI) to develop malware that can learn from its surrounding and acclimate to discover new susceptibilities.

(f) Attacks on connected vehicles put the brakes on the move by accessing connected systems, including those that control vehicles, invaders will result in accidents that threaten human life and disturb supply chains – not to mention effecting the status and income of automobile industry.

(g) Biometrics present a wrong logic of security Organisations will sleepwalk towards a weakening of access controls: biometrics will often be bargained by attackers who learn to discover gradually refined means to overcome them.

(h) New guidelines upsurge the risk and compliance problem Requirements for transparency will take to information being stored in several places and with third parties, increasing the probability of a data breach happening. At the same time, new data confidentiality principles will significantly rise the financial effect of a breach by imposing materially substantial penalties

(i) Reliable specialists reveal organisational weak points increasing stress on reliable professionals will lead some to disclose their organisation's weak points. Those entrusted with protecting data will be targeted or attracted to misuse their situation.

## III. CYBERSECURITY AND E-GOVERNANCE

As per Singh and Karaulia (2011) cybersecurity is usually concerned with information privacy, reliability and accessibility. It is also responsible to protect information, system and network against cyber threats. These characteristics reinforce services like verification of users, permission, accountability and reliability. In the wider perspective cybersecurity includes public and technologies both. Protocols of Information security have been established through the expertise of leading hi-tech nations and are easily available in the open literature [43]. For successful implementation of an information security framework these protocols frame various policies and procedures.

### *A. ICT and e-Governance*

Connectivity, knowledge, data content and capital are the four pillars of e-Governance [44]. ICT is responsible for connectivity and data transmission and storage. Therefore, in the era of Science, Technology and Innovation, effective use of ICT is vital to encounter the ever-growing outlooks of citizens and businesses. From mere computerization, e-Governance is constantly developing to offer access, fairness & empowerment to masses. Nagaraja (2016) defined "E-Governance" as the use of ICT to convert the usefulness, efficiency, transparency and responsibility of transfer of data and transaction between government, between government organisations, between government and citizens, between government and business. Through e-governance, government services will be made available to citizens in a convenient, efficient and transparent manner [12].

From study, it is established that most e-Governance initiative of ICT in developing countries fails and falls in two categories i.e. total failure which is 35% and partial failure which is 50% of ICT initiatives [36]. The writer points these facts to the difference among the present situation (environmental, social, fiscal and other conditions) and the structure of the ICT application - the larger the difference, higher the probabilities of failure. Safety has always been identified as one of the information system's key components. Contemporary information security management identifies compulsory to incorporate procedures and public including customary technology safety concerns, in guaranteeing information quality to every modern organisations. Significant technologies have already been invented to address major safety concerns. Still several operational issues, the public and procedural elements of information security management are yet to be addressed. This necessitates the socio technical system to aim on such problems in the mandatory framework for technically-emerging nations such as India. Generally, available publication understated ICT in developing states. Literature review establishes that there are universal recommendations of IT for e-Governance for developing nations but before assuming success of e-Governance factors supporting it required to be considered in respect of these nations such as their requirements and financial capacity. However, limited factual research is available publicly directly resolving these concerns.

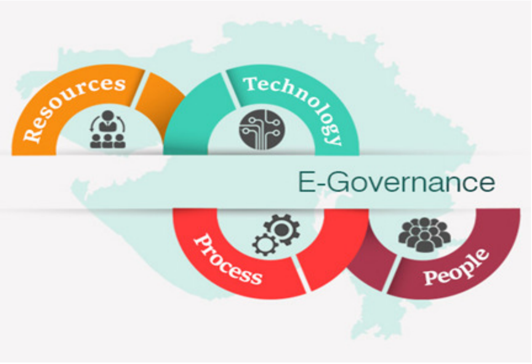

**Fig. 4.** ICT & e-Governance [37].

Therefore, protecting data and systems is of key importance since it can affect Governances' and users' willpower to follow the online services presented.

### *B. Applications of E-Governance in India*

E-governance provides government services to citizens in a convenient, efficient and transparent manner. Few of them are enumerated below [38]:

– Online applications and tracking.

– Online revenue records such as Khatauni, etc

– Form simplification and field reduction.

– Online repertories - Using e-repertories such as Digi locker (for certificates, educational certificates, ID cards, etc.) enabling public to use online valets as and when required to show/produce these documents to concerned.

– Unification of facilities and platforms e.g. Aadhaar platform of Unique Identity Authority of India (UIDAI), payment gateway, Mobile Seva platform etc.
– E-education: Provision of free Wi-Fi to every institute and offering Massive Online Open Courses (MOOCs)
– Healthcare Online: virtual medical advice, online availability of medical reports, online delivery of drugs, pan-India availability of patient records, etc.
– E-farming: getting instance price detail, placing order online and online receipt of money, advance, and getting relief compensation through mobile banking.
– E- security: online emergency services and calamity associated services through mobile instantaneously.
– E-payment: Internet banking, mobile banking, UPI, Bhim, Micro-ATM scheme and common service Centres/ Postal services.
– E-Judiciary: online Court services, e-Policing, e- Trials etc.

## IV. IMPACT OF CYBERSECURITY THREATS ON E-GOVERNANCE

E-Governance applications permit citizens and corporates to perform trade management online which couldelse need “a journey to business district”. Organisations are benefited, too, by means of reduced administration, better records, and improved efficiency [35]. Information and ICT can boost the reformation of task principles by helping various sectors, providing improved governance facilities to people, better governance dealings with trade and commerce, enabling citizen accessibility of data and involvement for policymaking and further resourceful governance administration. ICT effectivity in governance is prudently related to capability of Governance to inculcate a perception shift environment in organisations which is essential for transparent working and creation of expertise and its exchange. E-Governance leverages usage of digital technics to transmit and ensuring data to citizens and entrepreneurs. Nowadays, payment of water, electricity, telephone and any other types of bills is done online. Everyone is reliant on internet and when peoples depend on internet services all that come in e-Governance and any impact on IT/OT will definitely affect e-governance as it uses IT and OT infrastructure. The possible incidents an IT/OT network may face include the following:
– Choked or deferred movement of information through IT/OT networks [26, 27], which in turn could delayed e-governance services.
– Illegal modifications to commands, instructions, or alarm limits, that may harm, deactivate, or shutdown devices [26, 28], generate ecological effects, and/or jeopardize human life.
– Incorrect data sent to system operators, either to mask illegal changes, or to act the operators to initiate unsuitable actions [26, 28], which could have numerous undesirable effects.
– ICS software or configuration settings altered, or ICS software diseased with malware [27, 28], which could have several adverse effects on services rendered to citizens through ICS setup.
– Intervention with the functioning of protection equipment [27, 28], that may jeopardize human life.

## V. DISCUSSIONS

### *A. Key of Cybersecurity*

Cybersecurity, management level, is usually described in the form of few Trios [40] and based on these security experts define their goals and approaches accordingly. Bayuk (2010) defines the following three Trios covering best utilization of word are:
– “Prevent, detect and respond”
– “People, process, technology”
– “Confidentiality, integrity, and availability”
These echo the aims of cybersecurity, the method to accomplish cybersecurity, and the tools by which cybersecurity objectives are accomplished, respectively.

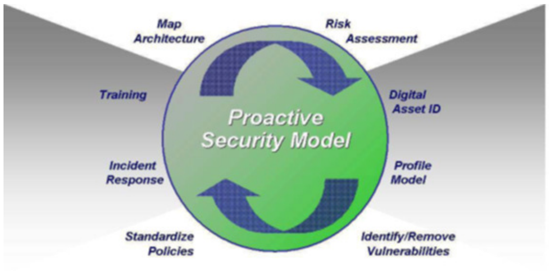

**Fig. 5.** Proactive security model [41].

Robust protection necessitates an elastic approach that permits adaptation to the varying atmosphere, distinct procedures and policies, the use of strong tools, and continuous alertness to provide reliable information accessible to needy public [42]. Assessment of the existing status of security of the installation is always beneficial to start security enhancement program. Authentic approaches to assess present state of security are available. Written down procedures and policies, and technology implementation are the integral part of a security program [42].

### *B. Security policy*

To be safe and sureis essential [42]. It is to be ensured that each security policy that is enforced by mechanisms is robust enough. To ensure comprehensiveness of security policies and make sure that they are totally enforced, structured procedures and risk assessment are available. A policy is a written down advanced strategy for whole organisation’s computer and information security. It offers an outline for taking precise decisions for example which defence tools to be used and how services are configured, and is the base for evolving secure software design rules and policies for network managers and operators to follow. Security framework is just broad specific guidelines and does not cover technology specific issues being a long term document such that [42]:
– Classification of acceptable users.
– Guiding principle to respond to compromised site.
– Advanced description of die technical atmosphere of the site, governing laws, procedural authority and the fundamental idea is applied while understanding the approach.
– Investigation of hazard detects installation’s resources, intimidations persistence against resources, and damage calculation of the resources.

– To formulate procedures for network managers to handle setups.

*C. Security Procedures*

Procedures are precise steps to be followed according to the IT security policy. Procedures talk about issues to recover programs through network, remote access of field equipment from home or on the move, use of encryption, validation for allotting accounts, programing, and supervision [14, 42].

*D. Security Practices*

Regular bombardment of spam, nowadays infected with zero-day malicious bouts, hazards of malevolent infiltrators, corrupted notebooks re-entering from the back of the packet examination firewalls and internet bouts protection devices are the reality of internet transmission nowadays. Statutory enforcement is required for hassle-free functioning, if not existing till now. Network management drills act an important task in system safety. General guidance including checklists for best safety conducts is easily accessible. Followings are some illustrations of typical suggested check lists [42]:

– Confirm each user has a PIN and the PINs should not be easily predictable. An OTP system is desirable.

– Usage of means like MD5 checksums (8, is a solid cryptographic method, to confirm the reliability of system software regularly.

– Use safe programming methods when designing software. These can be seen on the World Wide Web related to security sites.

–Be alert while online programing and doing modifications as you become susceptibilities.

– Frequently enquire with OEMs for the up-to-date available patches and keep systems healthy with updates and patches.

– Frequently verify available safety archives, such as those preserved by event response teams, for security warnings and technical information.

– Assessment of networks and systems, and often check logs. Various sites that agonize computer security episodes report that inadequate audit data is collected, so sensing and locating a cyber-attacks is challenging.

## VI. CONCLUSION

As McAfee stated in its Threat Predictions report 2016 [43], “Nation state cyberwarfare will become an equalizer, shifting the balance of power in many international relationships just as nuclear weapons did starting in the 1950s. Small countries will be able to build or buy a good cyber team to take on a larger country. In fact, cyberwarfare skills have already become part of the international political toolkit, with both offensive and defensive capabilities.”

It is apparent from above literature review that cybersecurity is an integral element of each e-governance drive. Digital security, operational secrecy and availability of data online are vital. In e-governance programs, security of governance policies and related critical documentations is required from illegal users. Above study shows that e-governance combined with security setups delivering appropriate safety is the prerequisite of any system design objective. Importance to be given to handle cybersecurity threats efficiently for effective e-governance to become India a progressive economy .It is the result of e-governance that today government is providing facilities to its citizen in effective and efficient manner. Due care to be taken in various executed e-governance projects like Digital India, Aadhaar, e-kranthi, etc. to make data reliable and secure. Yet, it still has some obstacles concerning e-governance, for example digital divide between rural and urban, illiteracy, poverty, safety and cost of execution, etc. These issues and challenges are having severe apprehension to government. Each government launched several initiatives by defeating the above problems and challenges. Further, each government must spend additional on these initiatives to make governance useful, transparent, accessible and safer in order to boost public confidence in good representative e-governance.

## VII. FUTURE SCOPE

Any study is not completely conclusive. Every study creates new scope than it covers. Following are some of the questions identified for future study:

– Cybersecurity and Digitization in India.

– Cyber Risk Assessment and its Mitigation aspects related to e-governance in India.

– Cybersecurity initiatives launched by Government of India and their effectiveness.

**Conflict of Interest.** It is confirmed that either of the author has no conflict of interest in publication of this paper.

## REFERENCES

[1]. Information Security Forum (2017). Threat Horizon 2019. Information Security Forum. Retrieved from https://www.securityforum.org/uploads/2017/03/ISF_Threat-Horizon-2019_Executive-Summary.pdf

[2]. Sharma, R. (2012). Study of Latest Emerging Trends on Cyber Security and its challenges to Society. I*nternational Journal of Scientific & Engineering Research*, *3*(6). Retrieved from https://www.ijser.org/researchpaper/Study-of-Latest-Emerging-Trends-on-Cyber-Security-and-its-challenges-to-Society.pdf

[3]. Rajaretnam, T. (2012). The right to consent and control personal information processing in cyberspace. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, 232 - 240.

[4]. Moore, M. (n.d.) Top Cybersecurity Threats in 2020. Retrieved from https://onlinedegrees.sandiego.edu/top-cyber-security-threats/

[5]. Consultancy.in. (2018). As India digitises, cyber crime is becoming an increasingly tangible threat. Retrieved from https://www.consultancy.in/news/1081/as-india-digitises-cyber-crime-is-becoming-an-increasingly-tangible-threat

[6]. Kumar, C. (2017, May 14). Ransomware attack hits at least 100 systems in India. Times of India, Retrieved from https://timesofindia.indiatimes.com/india/ransomware-attack-hits-at-least-100-systems-in-india/articleshow/58663696.cms

[7]. Indian Computer Emergency Response Team. (2018). Annual Report. Retrieved from https://www.cert-in.org.in/Downloader?pageid=22&type=2&fileName=ANUAL-2019-0123.pdf

[8]. NCRB. (2016). Cyber Crimes - 2014-2016. Retrieved from http://ncrb.gov.in/sites/default/files/crime_in_india_table_additional_table_chapter_reports/Table%209A.1.pdf

[9]. Tunggal, A.T. (2020, February 25). The 34 Biggest Data Breaches. Retrieved from https://www.upguard.com/blog/biggest-data-breaches

[10]. Paul, A., & Paul, V. (2011). UGC Sponsored National Seminar on Modern Trends in Electronic Communication & Signal Processing. In UGC Sponsored National Seminar on Modern Trends in Electronic Communication & Signal Processing (pp. 43–48). Piravom, Kerala: Excel India Publishers. Retrieved from https://www.researchgate.net/publication/306082683

[11]. Kumar, D., & Panchanatham, N. (2015). A case study on Cyber Security in E-Governance. *International Research Journal of Engineering and Technology*. Retrieved from https://www.irjet.net/archives/V2/i8/IRJET-V2I846.pdf

[12]. Nagaraja, K. (2016). E-Governance in India: Issues and Challenges. *IOSR Journal of Economics and Finance*, *7*(5), 50-54.

[13]. Pandya, D. C., & Patel, D. N. J. (2017). Study and analysis of E-Governance Information Security (InfoSec) in Indian Context. *IOSR Journal of Computer Engineering, 19*(01), 04–07. doi: 10.9790/0661-1901040407

[14]. Goswami, A. (2018). Impact of Cyber Security in different Application of E-Governance. *Journal of Advances and Scholarly Researches in Allied Education, 15*(4), 65–70. doi: 10.29070/15/57309

[15]. Shiels, Maggie (2011). Cyber War Threat Exaggerated Claims Security Expert. BBC Technology News, Retrieved from http://www.bbc.co.uk/news/technology-12473809

[16]. Brito, J., & Watkins, T. (2011). Loving the cyber bomb-the dangers of threat inflation in cybersecurity policy. *Harv. Nat'l Sec. J.*, *3*, 1-39.

[17]. Mills, E. (2011). Researchers Warn of SCADA Equipment Discoverable via Google. CNET News, Retrieved from http://news.cnet.com/8301-27080_3-20087201-245/researchers-warn-of-scada-equipmentdiscoverable-via-google/

[18]. Gorman, S. (2009). Electricity Grid in U.S. Penetrated By Spies. *Wall Street Journal,* Retrieved from http://online.wsj.com/article/SB123914805204099085.html

[19]. McMillan, R. (2010). Siemens: Stuxnet worm hit industrial systems. Computer World, Retrieved from http://www.computerworld.com/s/article/print/9185419/Siemens_Stuxnet_worm_hit_industrial_systems?taxonomyName=Network+Security&taxonomyId=142

[20]. Forum, E. (n.d.). Conficker infected critical hospital equipment: expert. Retrieved from http://www.electricityforum.com/news/apr09/Confickerinfectedcriticalequipment.html

[21]. Shachtman, N. (2017). Exclusive: Computer Virus Hits U.S. Drone Fleet. Retrieved from https://www.wired.com/2011/10/virus-hits-drone-fleet/

[22]. Zetter, K. (2017). Attack Code for SCADA Vulnerabilities Released Online. Retrieved from https://www.wired.com/2011/03/scada-vulnerabilities/

[23]. U.S. Dept. of Homeland Security. Industrial Control Systems-Cyber Emergency Response Team (ICS-CERT) Monthly Monitor. (2011). Industrial Control Systems-Cyber Emergency Response Team (ICS-CERT) Monthly Monitor: SCADA Hacking Using Internet Search Engines. Retrieved from http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Monthly_Monitor_Oct2011.pdf

[24]. Spiegel, R. (2019). 90% of Infrastructure Security Pros Have Been Hacked in the Last Two Years. Retrieved from https://www.designnews.com/design-hardware-software/90-infrastructure-security-pros-have-been-hacked-last-two-years/213044111660594

[25]. Top 10 Threats to Information Security. (2018). Retrieved from https://scsonline.georgetown.edu/programs/masters-technology-management/resources/top-threats-to-information-technology

[26]. Stouffer, K., Falco, J., & Scarfone, K. (2011). Guide to industrial control systems (ICS) security. *NIST special publication*, *800*(82), 16-16. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

[27]. Weiss, J. (2010). Protecting Industrial Control Systems from Electronic Threats. Momentum Press, ISBN: 1606501976 9781606501979.

[28]. Maynor, D., & Graham, R. (2006). SCADA Security and Terrorism: We're Not Crying Wolf, Retrieved from http://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf

[29]. Cai, N., Wang, J., & Yu, X. (2008). SCADA system security: Complexity, history and new developments. 2008 6th IEEE International Conference on Industrial Informatics. doi: 10.1109/indin.2008.4618165

[30]. Novealthy, M. T. N. (2015). Wearables and Quantified Self Demand Security-First Design. Retrieved from https://www.wired.com/insights/2014/10/wearables-security-first-design/

[31]. Sterling, B. (2012). Spear-phishing and Water-holing. Retrieved from https://www.wired.com/2012/10/spear-phishing-and-water-holing/

[32]. Krebs on Security. (n.d.). Retrieved from https://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/

[33]. Marcotte, R. (2013). Cybersecurity Lessons from the New York Times Security Breach. Retrieved from https://www.dlt.com/blog/2013/02/05/cybersecurity-lessons-ny-times-security-breach

[34]. Top 10 Threats to Information Security. (2018). Retrieved from https://scsonline.georgetown.edu/programs/masters-technology-management/resources/top-threats-to-information-technology

[35]. Information Security Forum. (2018). Threat Horizon 2020. *Information Security Forum*. Retrieved from https://www.securityforum.org/uploads/2018/03/ISF_Threat-Horizon-2020_Executive-Summary.pdf

[36]. Dada, D. (2006). The Failure of E-Government in Developing Countries: A Literature Review. The Electronic Journal of Information Systems in Developing Countries, 26(1), 1–10. doi: 10.1002/j.1681-4835.2006.tb00176.x

[37]. ICT & e-Governance. (n.d.). photograph. Retrieved from https://directorit.gujarat.gov.in/EGovernance

[38]. Singh, I. (2016). E Governance And Digital India. Retrieved from https://www.slideshare.net/InderBarara1/e-governance-and-digital-india-by-col-inderjit-singh

[39]. Patil, R. S. (2010). History and development of e-Governance. Retrieved from https://shodhganga.inflibnet.ac.in/bitstream/10603/2019/10/10_chapter-3.pdf

[40]. Bayuk, J. L. (2010). Triad and True. In Enterprise security for the executive: setting the tone from the top, 40–51. Santa Barbara, CA: Praeger.

[41]. Proactive security model. (2006). photograph, Idaho. Retrieved from 10.2172/911553

[42]. Singh, S. and Karaulia, D. S. (2011). E-Governance: Information Security Issues, *International Conference on Computer Science and Information Technology.*

[43]. McAfee Labs. (2015). 2016 Threats Predictions. Retrieved from https://www.intel.com/content/dam/www/public/us/en/documents/reports/mcafee-2016-threats-and-predictions-report.pdf

[44]. E-SPIN. (2018). Impact of Cyber Security in e-Governance: E-SPIN Group. Retrieved from https://www.e-spincorp.com/impact-cyber-security-e-governance/

[45]. Sangrola, H., & Palaria, R. (2017). E – Governance in India. *International Journal on Emerging Technologies*, 318–321. Retrieved from https://www.researchtrend.net/ijet/pdf/75-S-844.pdf

[46]. Talwar, M. (2015). Security Issues in Internet of Things. *International Journal on Emerging Technologies*. Retrieved from https://www.researchtrend.net/ijet/ijet61/65%20NCRIET.pdf

[47]. Kaur, R., & Singh, A. (2016). Cloud Computing Services Model and Security Threats. Retrieved from https://www.researchtrend.net/ijet/pdf/13%20IJET-SI-16.pdf

**How to cite this article:** Morya, K. K. and Singh, M. (2020). Study of Latest Cybersecurity Threats to IT/OT and their Impact on e-Governance in India. *International Journal on Emerging Technologies*, *11*(2): 939–947.