Information Security and Cryptography-Encryption in Journalism

Rajeev Ranjan Sahay

***Abstract:** The purpose of this review paper is to garner knowledge about the information security and cryptography encryption practices implementation for journalistic work and its effectiveness in thwarting software security breaches in the wake of 'Journalism After Snowden'. Systematic literature review for the 'information security and cryptography encryption in journalism' employed with an eye to synthesize existing practices in this field. For this, at first the existing approachable research article databases and search engines employed to download or get the abstract of relevant scientific articles which are then used for citation and summarization works in a systematic rigorous anatomization. Contingent upon them their analysis and synthesis employed to arrive at the findings. Research papers collated for the purpose of writing this review paper lighted up the vital issues related to investigative journalists' safety practices promulgation inadequacies even after the UNESCO 2017 and 2022 guidelines for urgent instrumentalization needs of journalists on the part of its' member States.*

***Keywords:** Information Security, Quantum Homomorphic Encryption, Encryption, Edward Snowden, Surveillance, Investigative Journalism.*

I. INTRODUCTION

Freedom enjoyed by the citizens in a country are the true parameter to gauge the level of freedom of expression guaranteed to them. The overarching canopy of the freedom of expression enshrine the freedom of the press and their duty to inform the public with spontaneity. Therefore, any enforcement or convulsion to the duty of journalists by any state/private actors are considered a threat to them. Today journalists underperform due to threats, affecting public need of information [1]. In the near past the digital attacks on journalists and in the aftermath their go missing in action cases has raised concerns towards gratuitous surveillance and necessitated the information security in journalism using encryption technology. Cryptography is the information security practice to convert soft plain information documents into soft cyphertext documents before online dispatch over internet. Encryption is the method to practice cryptography of soft plain documents. Today, no any academic institution/University wherein journalism is being taught as a vocational core curriculum, has arrangements to impart information security trainings either in project work format or as a major/minor electives/specialization. In this information technology society, it seems to be high time to include 'information security' in journalism course curriculums. Edward Snowden Revelation of the ramifications of mass covert surveillance of journalists has raised concerns among working journalists and rang them up to think about infosec practices in journalistic works. Coleman opine how in the wake of Snowden revelations, usage of infosec blockchain software applications like SecureDrop and Signal has increased since then by journalists [2]. Earlier almost everywhere due to the lack of the concern of the gravity of covert digital surveillance, infosec encryption seldom used in journalism. Coverage of encryption-related Leads increased after Snowden whistleblowing. The Cambridge Analytica Case of data manipulation and weaponization [3] after Snowden further aggravated concerns about infosec encryption promulgation in journalism. Recently, the Pegasus Spyware intrusion stings by Israeli software technocrats and foreign hackers turned the heads of newsrooms and journalists to become aware and vigilant of their own electronic gadgets being used for journalism [4], [5]. In recent years Journalist-Source communications has been put on the limelight due to increased government surveillance activities [6] and legal frame-ups against sensitive Sources in Britain and US as per Marimow, Savage and Kaufman [7]–[9]. The surveillance invisibility connoted for a "Black Box Metaphor" whose internal mechanism and threat level obscurity cannot be inferred because of dissimulation, inner elusiveness and multiform nature. European ICIJ investigative journalists vindicated that Information Security education & training is very important. Overall, a seamless umbrella approach to the study of digital threats to journalism is *erenata*. Surveillance being the rampant among the threats although not the only one. In a global scenario, with the rise of digital intelligence journalists are on the butt end and being harassed, mobbed, threatened, or go in a hush hush. InfoSec tools are being connoted for "Tools of Press Freedom". The English-speaking countries media outlets evangelically using SecureDrop as a whistleblowing platform software provider for keeping their Sources identity in disguise. SecureDrop usage in countries where journalism hasn't developed yet still need to be researched. For the Journalists working in "Free Press System" and in Authoritarian States there is a need to conduct research for Information Security gap studies.

Manuscript received on 18 July 2023 | Revised Manuscript received on 02 August 2023 | Manuscript Accepted on 15 September 2023 | Manuscript published on 30 September 2023.
***Correspondence Author (s)**

Rajeev Ranjan Sahay*, Department of Mass Communication and Journalism, Uttaranchal University, Dehradun (Uttarakhand), India. E-mail: rajeevranjansahay@gmail.com, ORCID ID: 0009-0004-8183-3078

Retrieval Number:100.1/ijmcj.A1047093123
DOI:10.54105/ijmcj.A1047.093123
Journal Website: www.ijmcj.latticescipub.com

Published By:
Lattice Science Publication (LSP)
© Copyright: All rights reserved.

A focused study of these dimensional variables is required to develop understanding about the amplitudes and potential differences. Amidst the persisting threats to the Source-cum-confidant privacy and digital-bashing of press freedom, journalists need to develop the skill to ensconce into these fluid and fragmented security culture to fill the gaps. There is a need of uniform information security culture for journalists [10]. Management of InfoSec is an abysmal and filibustered problem than is usually entertained and to hammer out solutions are likely to be achieved with acumen partially, while many *ex parte* and blinkered simplistic technical approaches are bound to founder. These awful backdrops have necessitated on the part of the engineers, economists, lawyers and policymakers to congregate and come under a brolly to try to forge common ground. Network hardware and software externalities, asymmetric nature of information, unpredictable moral hazard, adverse complaisant selection, vocational and avocational liability dumping and the "tragedy of the commons" are the key stumbling block inhibiting InfoSec infallibility [11].

Linux OS is an open-source software that is built on a multitasking, multiuser kernel offers web application security vis-a-vis to Windows. No system can be full-proof, however, switching-on adequate security options settings can sift web application communication over internet information exchange. The Amnesic Incognito Live System (Tails OS) is a Linux Debian-based distribution that offers anonymity, and surveillance-proof browser Tor for incognito web surfing and data exchange. Tor Web Browser is complementary software that run over Tails. Built over Linux kernel supports Android OS. TrueCrypt Data Encryption Tool originally embedded and bedecked with Windows/Mac/Linux now stands discontinued. VeraCrypt is offering services now instead. PGP Email Encryption is an integrated web service being offered for email point-to-point messaging security. Intel's Active Management Technology can become a target for running unsigned code hence exposing the system to malicious software infiltration. SecureDrop is a whistleblowing software written in Python for Linux based operating systems developed by Freedom of the Press Foundation for confidential communication between Journalists and their Sources. Signal Messenger App is multi-platform software developed by Signal Foundation for instant voice and video encryption and transmission. This review paper contributes to the readers through apprising them about the persisting limitations against gratuitous surveillance and ignorance of the freedom of expression by the state through dawdling investigations to nab the journalist-bashers. Section 1 provides a concise introduction about information security in journalism and the procedure for approaching to the relevant data, the number of research papers and books/articles referenced and their generalized findings. Section 2 deals with the significance of information security in journalism. Section 3 accommodate the types of information security. Section 4 deals with the application of cryptography in forensics journalism. Two emerging research areas namely infosec instrumentation, application and deployment-based research and Individual and organizational behavior-based research, are suggested for future researchers under scope of the study in section 5. Author’s recommendations are put in section 6 and finally section 7 concludes the review paper.

II. METHODOLOGY OF THE STUDY

In this section, the methodology of the study is detailed presented. In this study, the primary objective is studying the significance, application and limitations existing in the information security for journalism. On the basis of this objective, the author has applied Boolean Operators with search strings in the Search Engines of Scopus, google scholar and web of science. The keywords which are used in the Search Engines of Scopus, google scholar, IEEE explore, science direct and web of science for obtaining/identifying the different articles are mentioned in Table 1.

Table 1: List of Keywords and phrases used for literature search

Sl. No.	Keywords	Sl. No.	Keywords
1.	Information Security	2.	Information Security in Journalism
3.	Cryptography in Journalism	4	Encryption in Journalism
5.	Significance of Information Security	6.	Infrastructure based Security
7.	Types of Information Security	8.	Cryptography based security
9.	Scope of Information security in journalism	10.	Blockchain in journalism
11.	Quantum Cryptography	12.	Cloud computing in Journalism
13.	Application based security in Journalism	14.	SecureDrop
15.	Signal	16.	Edward Snowden
17.	Tor web browser	18.	Tails
19.	UNESCO report for journalism safety	20.	Visual cryptography in Journalism
21.	Homomorphic cryptography	22.	Quantum Homomorphic cryptography

After obtaining research articles from above databases, the next process is to select which articles need to be included and excluded in the study. The exclusion criteria are: the articles with no full text, the articles which are repeating with the same methodology, thesis and documentations of graduation, post-graduation studies. After selecting the articles, the number of articles which are included in the study are illustrated in Table 2. The year wise publications are detailed presented also we have mapped number of articles corresponding with their publication year-wise through color-band-coded format visualization. Color-bands in the beige, sky and light-pink for the duo collective multi-rows namely “No. of Articles taken” and “Year of publications” represents data for their respective columns co-relationally.

Table 2: Year-wise research articles used in this study.

No. of Articles taken	01	01	01	01	01	01	02	02	02
	03	01	01	01	05	07	11	09	07
	14	18	09	11	10	12	07		
Year of publications	1976	1978	1996	1998	2000	2001	2003	2004	2006
	2007	2008	2009	2010	2011	2012	2013	2014	2015
	2016	2017	2018	2019	2020	2021	2022	-	-

III. SIGNIFICANCE OF INFORMATION SECURITY IN JOURNALISM

Information protection has been the core collective unconscious journalistic practice in journalism by convention. Being the 'fourth estate' (as coined by Edmund Burke) has tried to maintain the economic and government balance of power of the state [12], [13]. This watchdog role has contributed to the accountability enforcement on the part of the government to ponder, plan and purge with the persistent inconsistency stumbling blocks for inclusive development of the state. Hence, work towards informed, infrastructure and inclusive blasé public that exhibit their power through righteous voting discernment to elect accountable representative to the governing chair. *Laissez faire* working environment with autonomy to communicate with their confidant Sources to bring to the public gaze mirror image of political developments, are crucial as Budarick and Waisbord avers, the socio-political autonomy of the press is crucial to supersede economic and political pressure exercised by state actors and institutions with whom most of the resources befall [14], [15]. In the wake of the covert mass surveillance revelation by the former NSA contractor Edward Snowden, a groundswell of unrest has ensconced about getting tracked on job and forceful incommunicado. Moreover, trails of metadata surfing history of internet can best be used to track journalists and their confidants/sources without formal subpoena against them by the state. Hence, "to defeat surveillance and prosecutorial intrusions and to strengthen the rights of journalists before the courts … it is essential that journalists update their own rules and norms for the age of surveillance" [16]. Contemporary technology of public surveillance exacerbates the problem and can be misconstrued as ad hoc guided surveillance against journalists as does collection of 'data doubles' due to continuous identical data feeds that connotes to the concept of "Surveillant Assemblage" by Haggerty and Ericson [17]. Shifting from a surveillance society to a surveillance culture where mass surveillance is legit by government, it becomes imperative on the part of journalists to commit for themselves and their confidants/sources privacy. Infringements to journalists' privacy in galore reported in yesteryears that include data interception, interpolation and unauthorized retrieval gave groundswell of chilling effects of such threats that rung funky frisson of Sources demur to go hand in glove with their guy Journalist. Pew Research Center disclosed the fact that decreasing resources at hand in newsrooms and Journalists' sporadic usage of Infosec tools to dodge interception and surveillance has contributed to go *sang-froid*. Most of the journalists despite getting adept to use infosec tools namely TLS and Signal, their metadata trails over internet in the form of browsing time, workstation IDs, location and communication data size can be misused by malefactors to tap unethical and illegitimate business needs. XRD is a point-to-point metadata private messaging system that hides users' identity through mixing messages in mix-chain pooling servers before delivering to the end-users' mailboxes [18]. The XRD architecture given in Figure.1 below comprises of users, mix-chain servers and the mailbox servers. Each user choses a discrete random chain of servers having at least one honest server with overwhelming probability for their shuffled messages routing over networked servers that drop messages in users' mailboxes eventually. Due to shuffling messages over mix-chain servers, users' metadata remain unidentified.

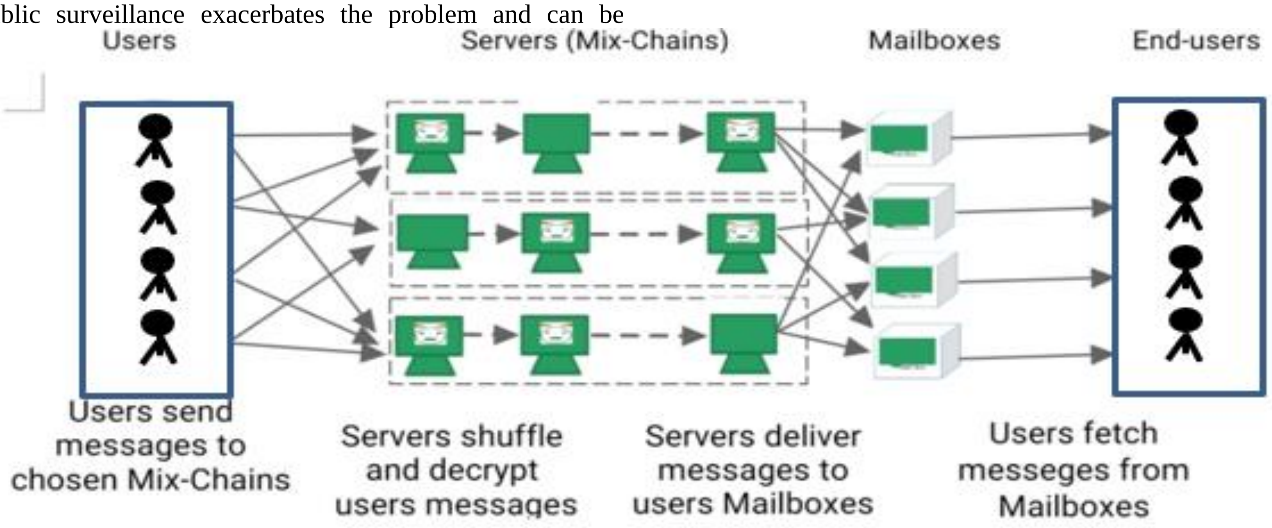

Users
Servers (Mix-Chains)
Mailboxes
End-users
Users send messages to chosen Mix-Chains
Servers shuffle and decrypt users messages
Servers deliver messages to users Mailboxes
Users fetch messeges from Mailboxes

Figure1: Overview of XRD Operation

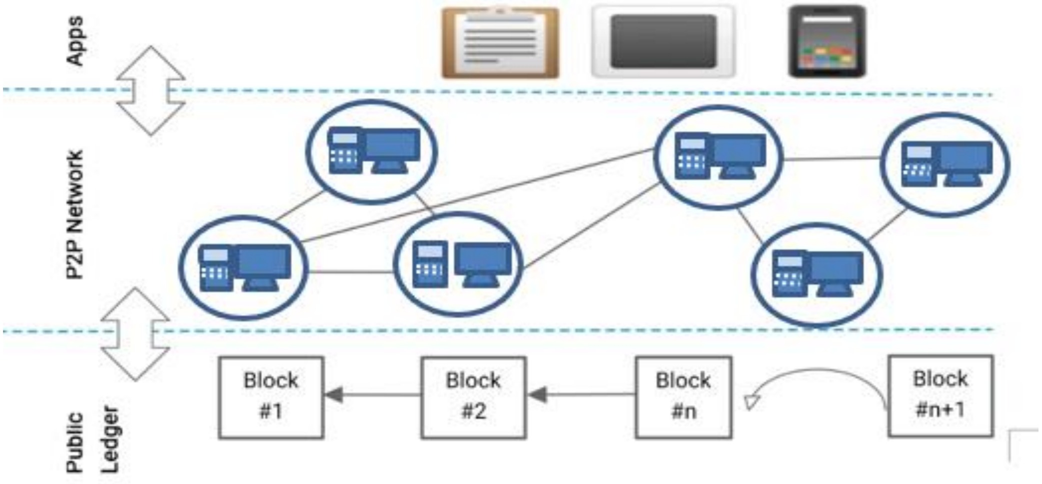


Figure 2: Structure of Blockchain

Resolving conflict of interests arising due to leakage of whistleblowers information, Tomaz [19] proposed a blockchain utilizing ring signature scheme to authenticate the participants anonymity and its' revocation whenever required by the participant, as the case may be.

Table 3: Literature suggesting significance of Information Security in Journalism

Author (s) & year	Findings
R. Anderson [11]	Network hardware and software externalities, asymmetric nature of information, unpredictable moral hazard, adverse complaisant selection, vocational and avocational liability dumping and the "tragedy of the commons" are the key stumbling block inhibiting InfoSec infallibility.
J. M. Anderson [20]	This article is suggestive of the need on the part of InfoSec professionals to do the perfect segmentation of their work area as per InfoSec requirements.
S. E. Chang *et al* [21]	A business firms' prime requirement is to have an umbrella information security and practices management.
K. J. Knapp *et al* [22]	Supraordinate management camaraderie and support is very crucial for an information security program and policy.
J.-N. Ezingeard *et al* [23]	Superordinate management acumen, buttress and evangelical support vivify timely upgradation of information security systems.
J. Aycock *et al* [24]	This is the systems requirement to track users for persistent state management activities. However, users need to be aware of these innocuous but not insidious back-ends.
B. A. Forouzan [25]	Cryptography technicalities are mentioned that is a must read for getting expertise in InfoSec.
S. Baack [26]	Among all sensationalized eruption in the field of journalism in the wake of 'leaks' culture, I opine that normalized journalistic practices sustain the budge by dint of its gatekeeping credentials.
B. Brevini [27]	The article deals with dialectical pros and cons for 'Leaking to Public' strategy adopted by Assange.
B. Alfter [28]	Cross-border Journalism is the demand of the hour for beats related to trans-border international concerns including human rights. Prescribing methodology for this.
P. Di Salvo [29]	In this Information era, information protection is paramount on the part of a journalist to sustain in the competitive environment.
P. Bradshaw [30]	In want of technological and legal dearth of knowledge journalistic practices suffer a lot. Improvised training ought to be given to alleviate this insecurity.
R. Abu-Salma *et al* [31]	Due to lack in the sketching of users' mental model and inefficient security tools ergonomics as per their contextual needs for them.
J. Angwin [32]	Cub-reporters need to be familiarized with InfoSec tools usage.

B. Ataman [33]	This article focuses on the state oppressive policy adopted by Turkey for the maintenance of state hegemony over media.
M. Crete-Nishihata *et al* [10]	There is a need of Uniform Information Security culture for Journalists.
P. Di Salvo [34]	SecureDrop usage in countries where journalism hasn't developed yet still need to be researched.
P. Di Salvo [34]	European ICIJ investigative journalists opined that Information Security education & training is very important.
J. R. Henrichsen [35]	With increasing institutionalization of SecureDrop in newsrooms, homogenized journalistic practice will grow on its own.
L. Tsui *et al* [36]	This article provides InfoSec practices by journalists working either in China or Hong Kong. But do provide ballpark estimate of the fate of journalistic practices in other parts of the world in want of adequate InfoSec Tools.
P. Di Salvo [37]	InfoSec tools are being connoted for "Tools of Press Freedom".

Along with the significance of information security, in the table 4, we have discussed the different studies that discuss about the information security policy, awareness and training. The findings of each study are summarized in the table 4.

Table 4: List of articles on information security policy, awareness and training.

Author (s) & year	Findings
M. E. Whitman [38]	Amidst disruptive airing of threats & breaches to information security blitzkrieg in the press there is a vital highbrow need to plug the loophole through awareness, education and policy.
J. M. Hagen *et al* [39]	Non-technical measures of information security awareness-creation found to be a bolster in comparison to the techno-administrative ones.
S. Carlo *et al* [40]	This is highbrow detailed training kit for all practicing journalists.
J. Angwin [32]	Cub-reporters familiarized with InfoSec tools usage.

IV. TYPES OF INFORMATION SECURITY IN JOURNALISM

A. Application Based Security:

With the growing mediatization and datafication of society and journalism through media technology applications, surveillance and privacy related issues are on the hike posing security threats. Usage of Artificial Intelligence in Journalism for contents robotization is the recent application software advancement that intake well tabulated data feed to generate automated mechanized full proof contents for publication, independent of humanoid literature, for many, this has felicitated the professions' drudgery.

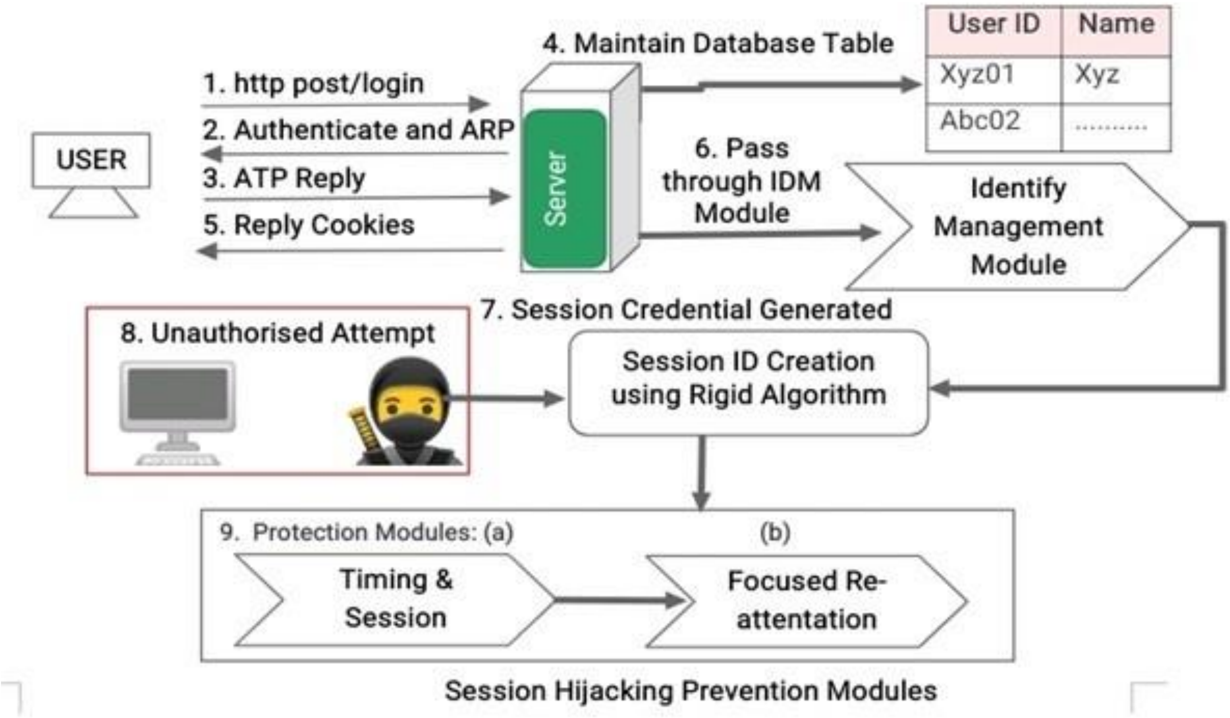

USER
1. http post/login
2. Authenticate and ARP
3. ATP Reply
5. Reply Cookies
Server
4. Maintain Database Table
User ID
Name
Xyz01
Xyz
Abc02
....
6. Pass through IDM Module
Identify Management Module
7. Session Credential Generated
8. Unauthorised Attempt
Session ID Creation using Rigid Algorithm
9. Protection Modules: (a)
(b)
Timing & Session
Focused Re-attentation
Session Hijacking Prevention Modules

Figure 3: General Architecture of session hijacking

Retrieval Number:100.1/ijmcj.A1047093123
DOI:10.54105/ijmcj.A1047.093123
Journal Website: www.ijmcj.latticescipub.com

Published By:
Lattice Science Publication (LSP)
© Copyright: All rights reserved.

Web application, Mobile and Application Programming Interface (API) related security breach vulnerabilities are the prime areas under InfoSec remediation for data-based journalism. Toolkits namely RIG and Sundown used for vulnerability attacks through SQL Injection and Cross-site Scripting (XSS) can be averted using VulScan software. Session ID hijacking is web application security breach perpetuated using tools namely T-Sight, TTY Watcher, Hamster and Ferret, Wire shark, Ethereal, Juggernaut and Hunt *et cetera* which can be averted through session ID creation using strong long random alphanumeric character algorithm, time-out sessions and forcing re-authentication.

B. Vulnerability Management

Risk reduction is the prime target of Information Security Management System. The relationship among asset, threat and vulnerability as shown in Figure.4 below guide to frame the probable targets of evaluations (TOE) as shown in Figure.5 *ut infra*.ISO/IEC 19791 is the standard for operation environment security assessment (Figure 5).

Contingent upon the inter-relationship among assets, threats and vulnerabilities the Common Criteria (CC) has proposed the InfoSec functional requirements relationship with the InfoSec security objectives for the target of evaluation (TOE) as shown in Figure.5 *ut infra*. Together the InfoSec security functional requirements along with the InfoSec security assurance requirements confer the protection from ISMS vulnerabilities and threats. The CC proposed framework for the ISMS shown in Figure.6 *ut infr*

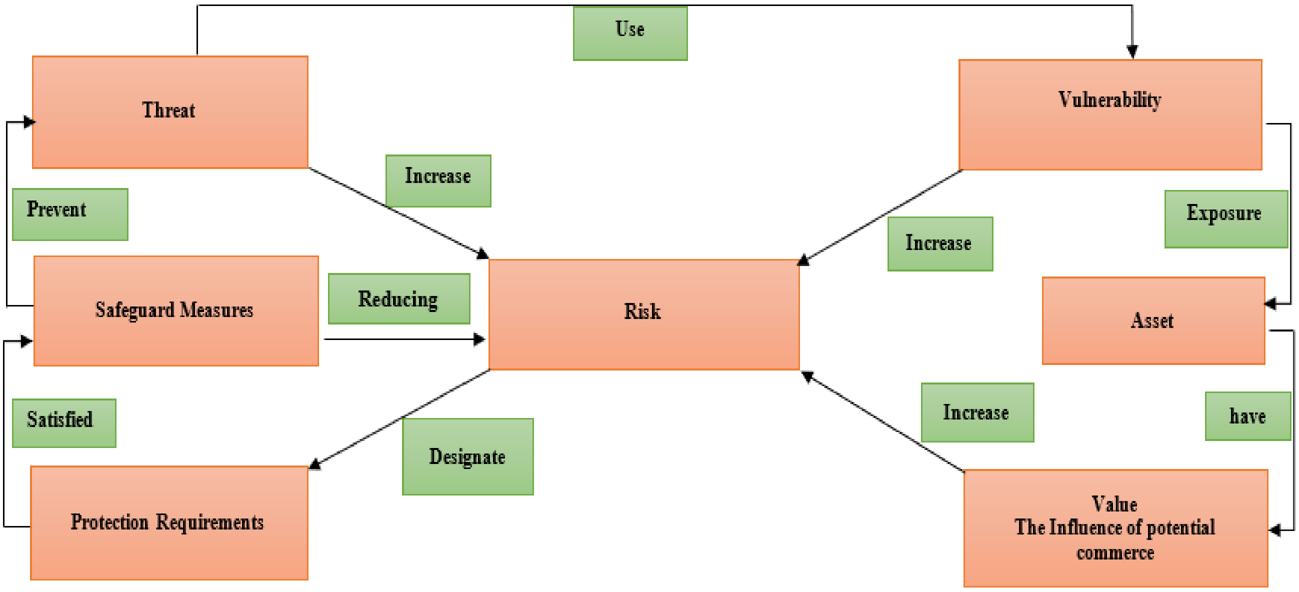


Figure 4: ISMS risk component flowchart and relationship (ISO/IEC TR 13335-1)

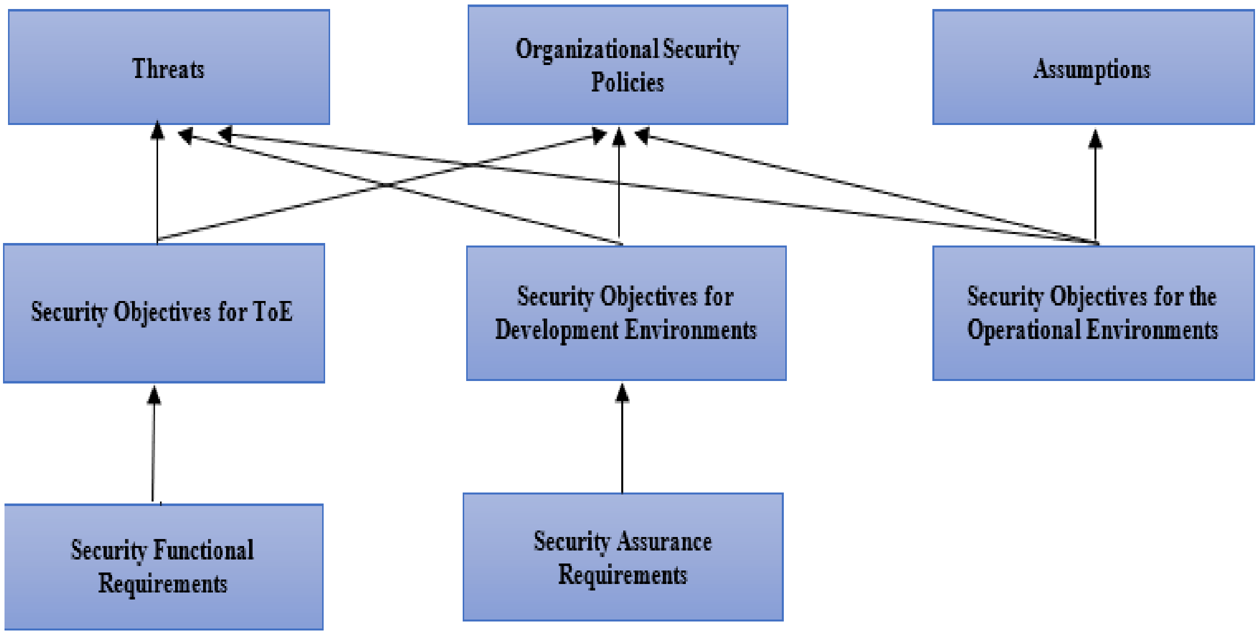

Threats
Organizational Security Policies
Assumptions
Security Objectives for ToE
Security Objectives for Development Environments
Security Objectives for the Operational Environments
Security Functional Requirements
Security Assurance Requirements

Figure 5: Relationship between security objectives and requirements

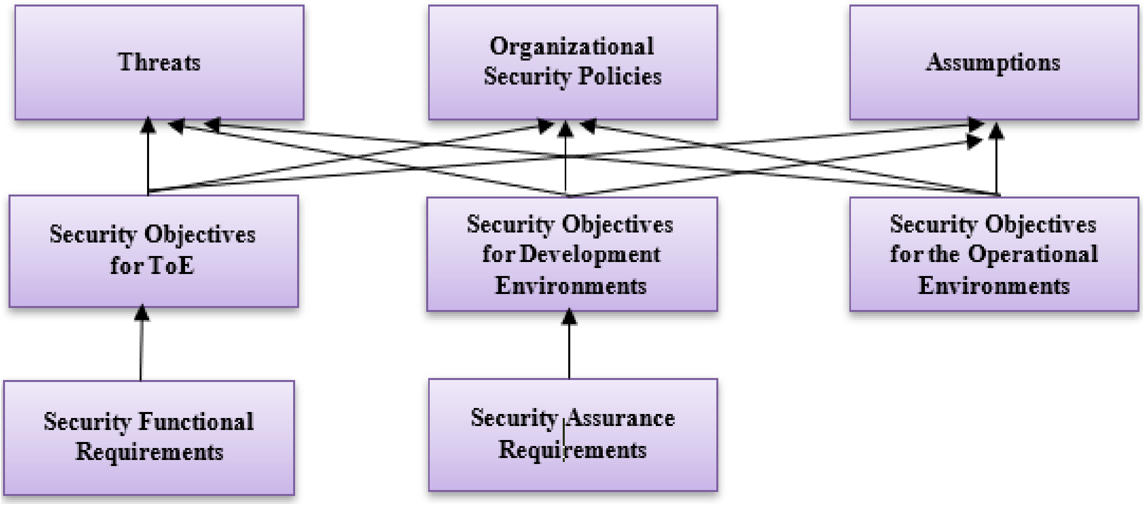

Threats
Organizational Security Policies
Assumptions
Security Objectives for ToE
Security Objectives for Development Environments
Security Objectives for the Operational Environments
Security Functional Requirements
Security Assurance Requirements

Figure 6: Framework of Information Security Management System (ISMS)

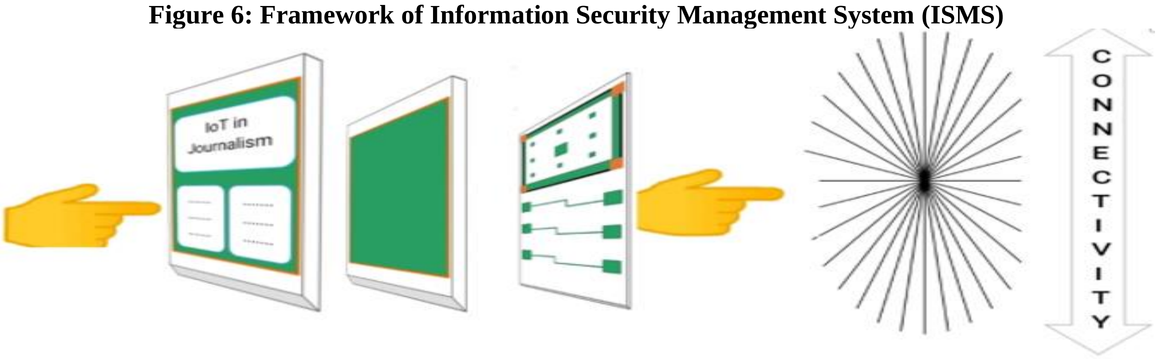


Figure 7: IoT based Online News Media

C. CLOUD BASED SECURITY

The National Institute of Standards and Technology (NIST) define Cloud Computing as an open on-demand service model to public for the usage of large pool of interconnected and distributed computing resources that can be employed or released with a minimal effort of the management and cloud services providers, facilitate Software-as-a-service (SaaS), Infrastructure-as-a-service (IaaS), Platform-as-a- service (PaaS), Virtualization, Computing-as-a-service (CaaS) and Security-as-a-service (SECaaS).

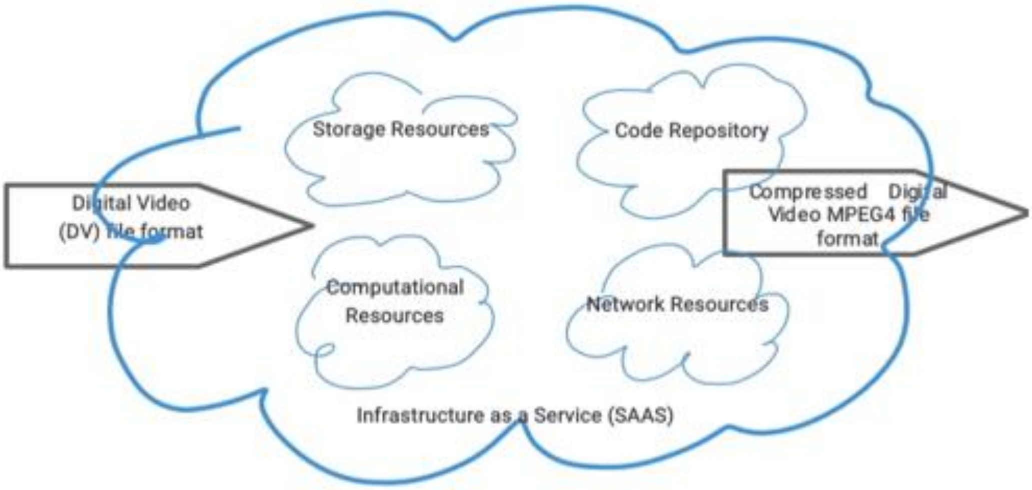

Storage Resources
Code Repository
Digital Video (DV) file format
Compressed Digital Video MPEG4 file format
Computational Resources
Network Resources
Infrastructure as a Service (SAAS)

Figure 8: Cloud Computing Platform

Internet-of-Things (IoT) is the connectivity of physical things with internet to control the remote operation and interconnectivity with other online devices. IoT based security threats includes (1) Threats to Information viz. personal data, biometrics data, geolocation data and diurnal activity data etc. (2) Legal threats viz. data retention laws, injunction from strong encryption, criminalization of whistleblower activities and dubious data regulations etc. (3) Physical threats to Journalists viz. IoT sensors in electronic gadgets (4) Threat vectors of IoT devices viz. reuse of code libraries, password insecurity and firmware upgradation problems (5) Privacy threats viz. data capitalism and insufficient industrial regulations and (6) Access control related threats viz.

Retrieval Number:100.1/ijmcj.A1047093123
DOI:10.54105/ijmcj.A1047.093123
Journal Website: www.ijmcj.latticescipub.com

Published By:
Lattice Science Publication (LSP)

data output from IoT devices manipulation. In several industries including media and telemedicine audio-visual video File formats now-a-days taking services of Infrastructure as a Service (IAAS) cloud computing to upload bulky video Files onto cloud (Meghdoot, in India, an open-source cloud stack) and using SAAS compression services to deliver compressed MPEG4 video Files over internet destinations as given in Figure.8 *ut supra*.

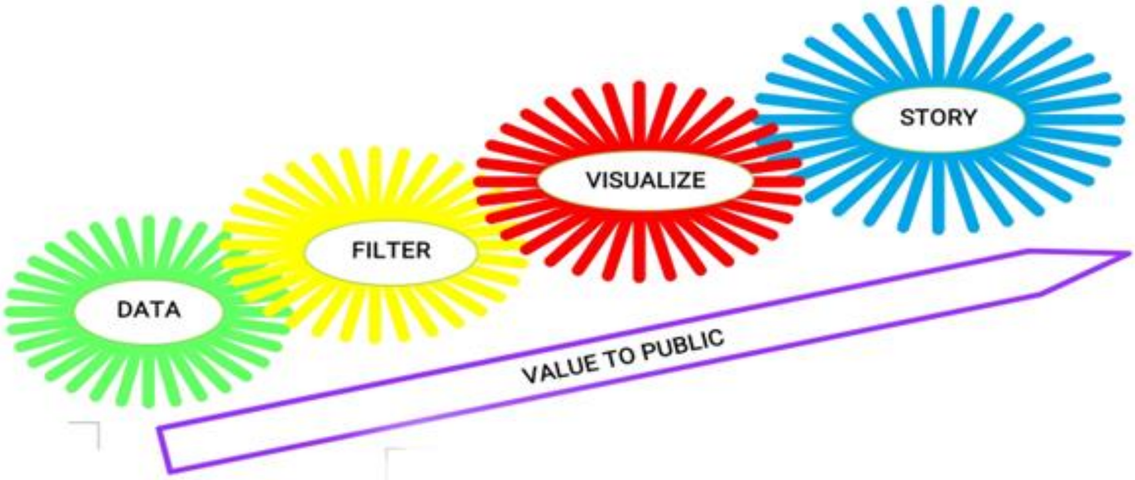


Figure 9: The process chart for visualizing data-mining

Data driven journalism incorporate visualization of data mining over cloud through exploring, displaying and expressing data meanings by means of visual communication that transcend the barriers between information communication and communication as given above in Figure.9 Another cloud application is secure mobile payments over cloud, a run-of-the-mill issue now-a-days because Europay MasterCard Visa (EMV) application provider third parties' role substituted with the trusted cloud payment applications stored in the cloud. Compelled disclosure to the government, data security and disclosure of breaches, data availability and data localization are among the privacy issues of cloud computing whereas client-server security, location and control of data, network security (DNS Attack, Sniffer Attack, Issue of reused IP Addresses, Denial of Service, Distributed Denial of service and DBGP prefix hijacking etc.) data recovery in the cloud computing, securing data on cloud, installation and maintenance of firewall, data encryption and back-up & recovery issues are among the cloud security services.

D. Cryptography based Security

Cryptography is the practice of using information security techniques to secure data, information and messages from third-party interception. The focal areas of modern cryptography information security in different fields include information confidentiality, integrity, availability and non-repudiation. Algorithms

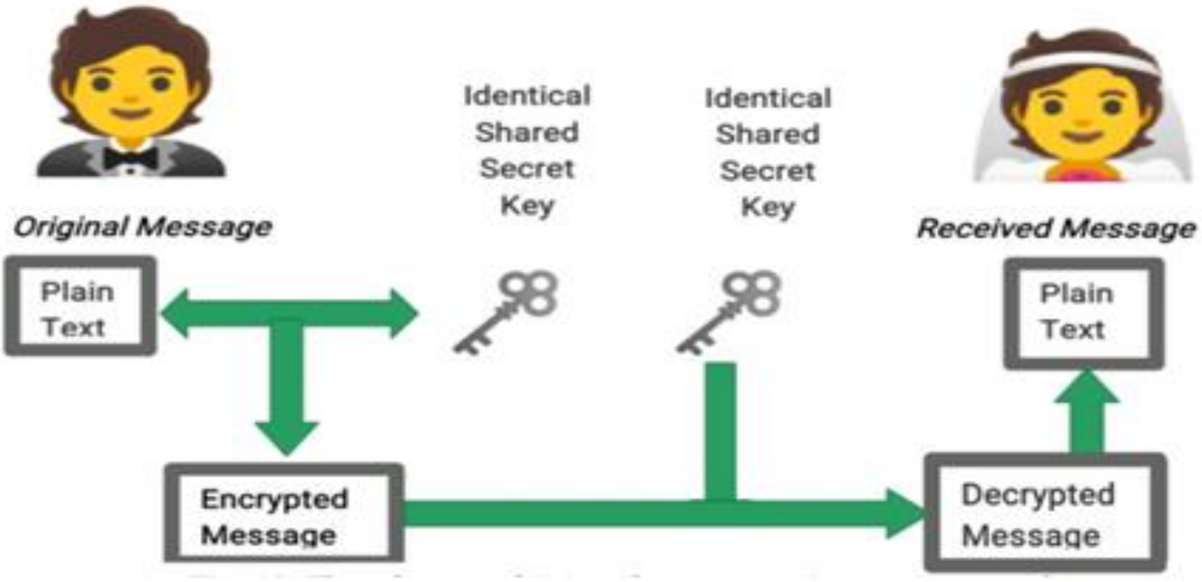


Figure 10: Flowchart explaining the symmetric encryption schemes.

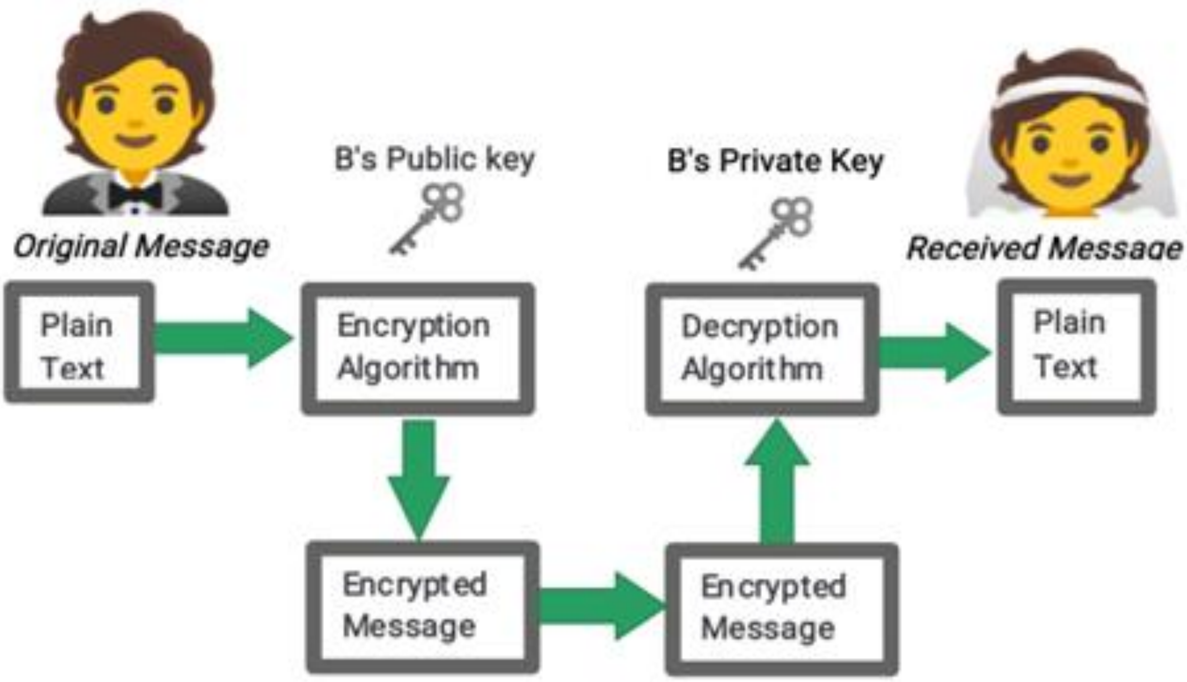


Figure 11: Flowchart explaining the asymmetric encryption schemes.

to implement cryptography are Data Encryption Standard (DES), Advanced Encryption Standard (AES), Identity Based Encryption (IBE) and Rivest, Shamir, Adelman Algorithm (RSA). Asymmetric encryption method in Figure.11 requires a pair of keys, public and private keys, for each party involved in online communication whereas symmetric key cryptography in Figure.10 use identical single key exchange between parties for communication.

Quantum computing is getting on an even keel with every passing day making the traditional asymmetric key cryptography and to a moderate extent symmetric key cryptography also, obsolete

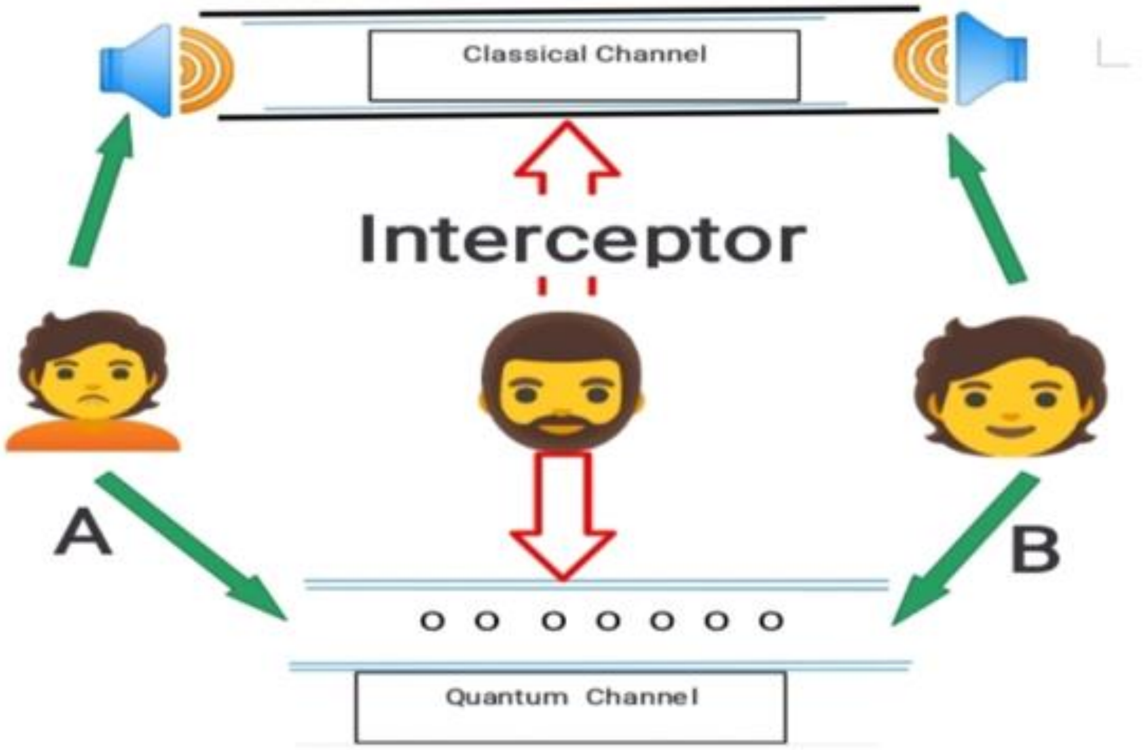


Figure 12: QKD Model for BB84 protocol

Retrieval Number:100.1/ijmcj.A1047093123
DOI:10.54105/ijmcj.A1047.093123
Journal Website: www.ijmcj.latticescipub.com

Published By:
Lattice Science Publication (LSP)

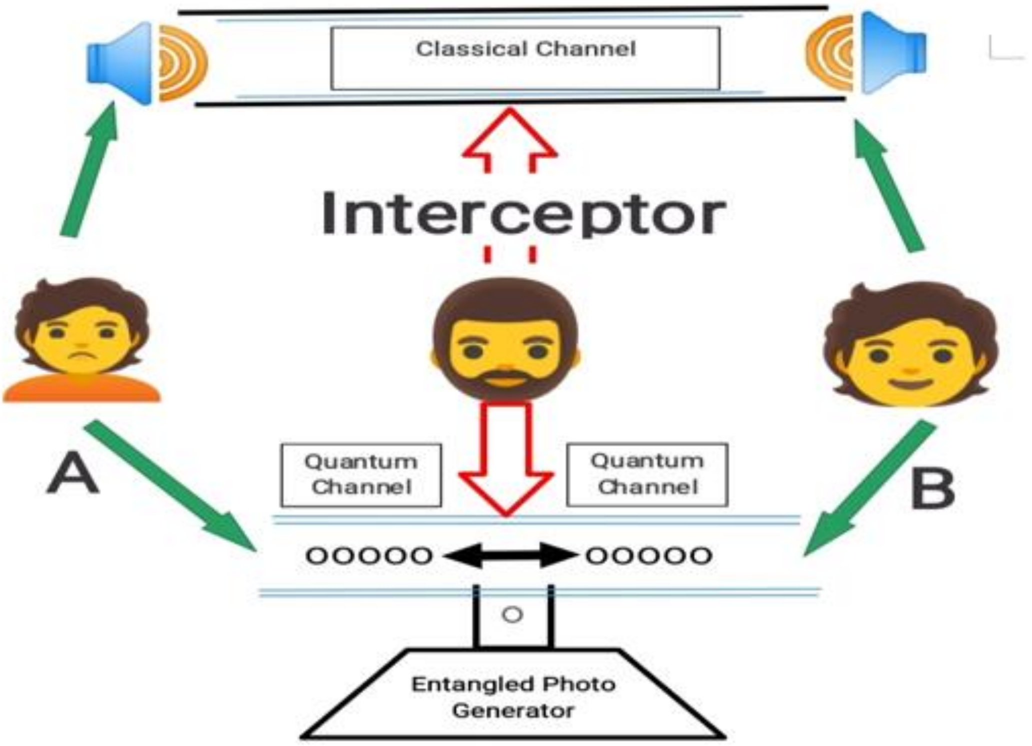


Figure 13: QED Model for Eckert's protocol

because the basic algorithmic bedrock namely RSA, DSA and blockchains' existing mathematical foundation (elliptic-curve discrete logarithm problem, integer factorization problem, the discrete logarithm problem) are easily bypassed using quantum computers.

E. Infrastructure based Security

Talking about infrastructure-based security in journalism, it comprises of device-based security, media-based security and infrastructure system hardening. Device-based security includes Firewalls, Router, Switches, Modem, remote access service (RAS), Telecom/Private Branch eXchange (PBX), VPN, IDS, Network Monitoring/Diagnostic, Workstations, Servers and Mobile devices *et cetera*

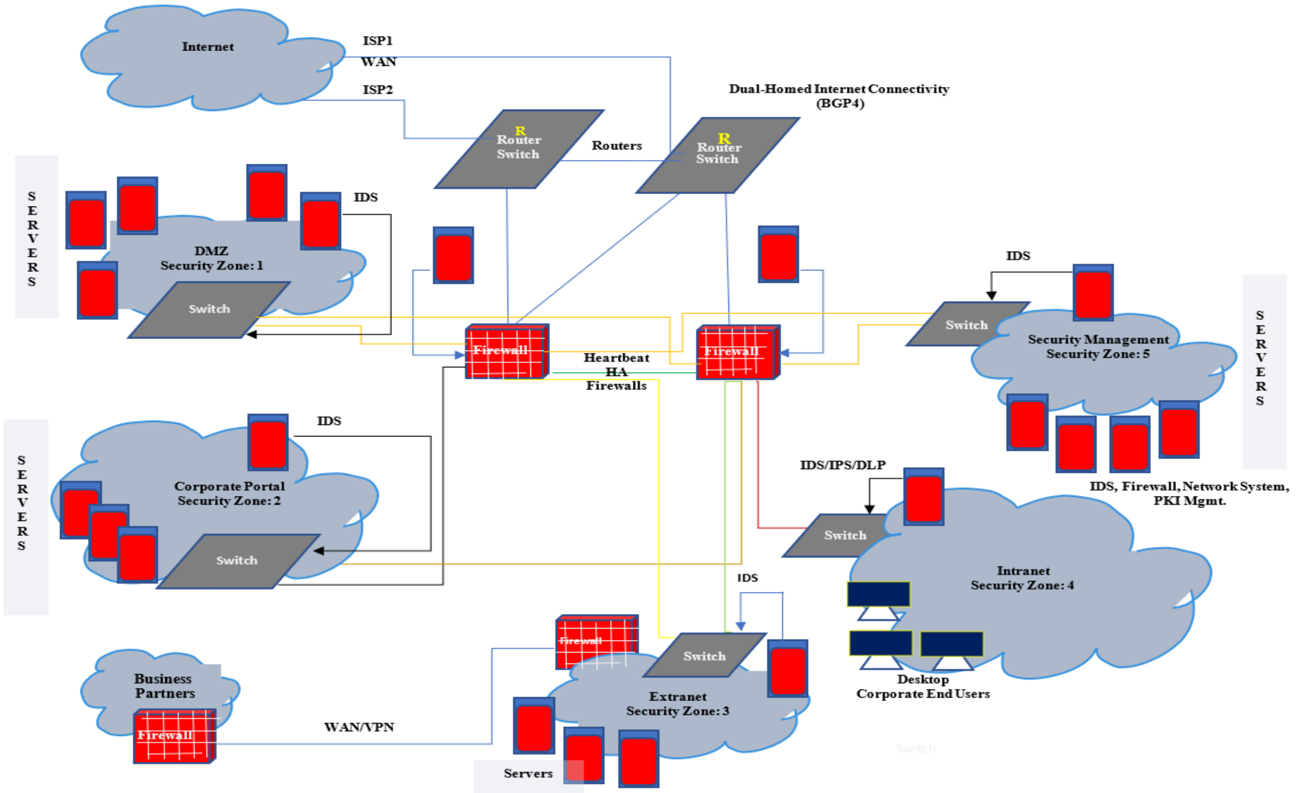


Figure 14: Secure Extranet and Private Cloud

Media-based security includes Coax, UTP/STP, Fiber Optic, Removable Media, Magnetic Tape, CDRs, Hard Drives, Diskettes, Flashcards, Smartcards and the rest. Infrastructure-system hardening requires OS-hardening, Network-hardening and Application-hardening. Henrichsen, Betz, and Lisosky's UNESCO study in 2015 for digital journalism safety identified twelve (12) key infrastructure-based threats viz. illegit digital surveillance; non-ergonomic digital safety tools; expensive digital security tools; open source digital security tools lacking sustainable business model; denial of service attack; unawareness of available technological digital security tools; unawareness of data anonymizing encryption tools; safety of data documentation against digital threats unavailability; location tracking technologies by state and non-state actors to track the journalist and their sources identity; phishing campaign, compromised user accounts and devices and digital security teaching and training for journalism not being taught in a systematic and holistic way. For tackling such socio-technological issues, newspaper publishers and IT companies have collaboratively made headway for new tools and methodologies incorporation into journalistic practices through fact-checking software. International Consortium of Investigative Journalists (ICIJ) with the aid of Swiss University EPFL has developed a Datashare platform for reporters around the world to navigate and share documents of their use required for investigations. At the intersection of emerging cutting-edge technologies and safety culture infrastructure for journalism, transdisciplinary research incorporating qualitative methodologies and advanced technological approaches, is required. Development of effective enterprise information infrastructure, IT infrastructure management and business & IT alignment are some key management activities required exigently to have ace impact to enhance the quality of information security management.

D. Incidence Response based Security

Incidence response-based security is an enhanced management skill that enshrine early earnest monitoring and detection of comprehensible breaches in computer local and network security and their timely response to plug and clog the jugular loopholes. With the growing interest in cyberspace security and the inherent development that has grown from undercover hacking activities to a semi-covert government surveillance, tracking and spying, the need for an enhanced incident response-based cybersecurity neural networks with visual analytics is afoot now. Eric Butlers' Firesheep, an add-on to the Firefox web browser host unencrypted data-transmission facilities for end-users to monitor data-traffic over public Wi-Fi made the social media (Facebook & Twitter) platforms' owners to switch over to enhanced https-based log-in substitute for their app-users. Photobucket, for an online photo-sharing platforms' Fusking/Fuskering Achilles' heel that exposed users' private photo-files, taking recourse of scrambled URLs and *ad hoc* privacy settings. Macintosh Apples' iCloud service that facilitates its users to sync their pictures, documents and other contents across all their Apple devices, doped for Mat Honan, a Wired.com journalists' user account unauthorized access by Grey-belt hackers for Mat regret had he adopted creating (a) routine back-ups, (b) using two-step Google authentication and (c) keeping a separate unshared recovery address, he could've avoided the ditch doping attempt. Social Media companies while preparing their incidence-response strategy can infer/learn from common end-users' behavior to fortify and bolster security accessibility. LinkedIn 2012 user-accounts password leaks by the Russian-language forum made the company to bite the bullet through letting reconfiguration of the passwords at the user's end. Similarly, eHarmony too bolstered their platforms' users-accounts personal information by using hashing and encryption techniques and switching over to SSL/Firewalls. Sony PlayStation Network's negligence in transparency and timeliness non-response in the wake of its' platform's user-accounts data breaches forced the company lagged behind others. Indian Computer Emergency Response Team (CERT) on January 20, 2021 has issued an advisory against the rising data-security breach activities as a proactive measure curbing these online vulnerabilities, a hardliner against malefactor going with impunity. Raju and Geethakumari studied the security and intruder detection-handling process of cloud computing and proposed an intrusion incident detection algorithm to collate intrusion-data that can be legally used in the Courts of Law.

1. Cryptography in Journalism

According to Snowden, the global surveillance disclosures provided "irrefutable evidence that unencrypted communications on the internet are no longer safe", and therefore in his view, "Any communications should be encrypted by default" (Snowden, cited in The Guardian, 17 July 2014). Studies about Journalists around the world for their lack of knowledge to incorporate and integrate digital security measures while practicing digital journalism and to provide carapace to their sources have been undertaken by many namely, report in UNESCO for their International Survey of Journalists'; Posetti [41] reporting about how to protect journalism sources in digital environment; Kleberg [42] digital source protection; Bradshaw UK regional digital journalism source protection; and Lashmar [43] interviews with Journalists from countries of the Five Eye alliance services (Australia, Canada, New Zealand, UK and USA).
Crypto-AG, the world's largest crypto-machine factories in collusion with their ally a code-breaker William Friedman in 1950 connived to leak encryption in their devices deliberately to funnel vital aces to Washington and other allies to sniff and read messages. This goes by the codename appellations 'Thesaurus' or 'Rubicon', was one of the sensational security breaches since WWII Bletchley Park operation that decrypted and thwarted Axis communications. The Global South States suffered most due to this. The 'Wired' magazine in 1993 for its' second edition cover page frontispiece billed the three founding members of cyberpunk movements namely Timothy C. May, Eric Hughes, and John Gilmore holding in their hands the Stars and the Strips with the caption 'Rebels with a Cause (Your Privacy)' for a cover story 'Crypto Rebels'.

Digital transformation of Investigative Journalism has opened vistas for encryptable, manipulable, tampered with and decentralized information that mandated fabrication and adoption of sophisticated software and mindsets to make headway to beat disruptive tendencies. Data Journalism sites namely Vox, FiveThirtyEight and Quartz and its' inclusion into Journalism education shows how Words and Statements, Digital Photos and Videos are abstracted and archived as data in spreadsheets. Image forgery detection to trap the duplication of image is performed through online services of *Google Image* and *TinEye* for social media content verification. Metadata for Social Media Forensics is not adequate and utilizes services of *Imageforensic* or *Reveal* and on-premises tools namely *Ghiro*, *Jpegsnoop* and *Phoenix*.

Edward Snowden revelations results in frisson amongst investigative journalists to adopt the new normal through 'Going back to the Analog' and farm out and outsource services of information clearing houses like International Center for Investigative Journalists (ICIJ).At present Digital Image Forensics incorporate digital signatures and Digital Image Watermarking to investigate image forgery which provide image authentication and certain image integrity only that can be applied during image capturing and storage for image ownership authentication Figure.15 .

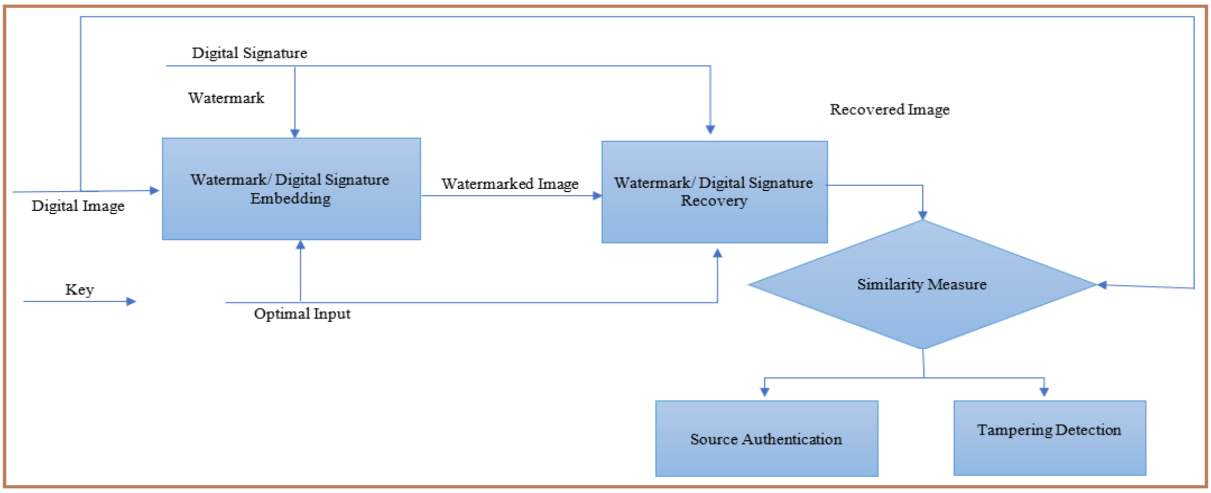


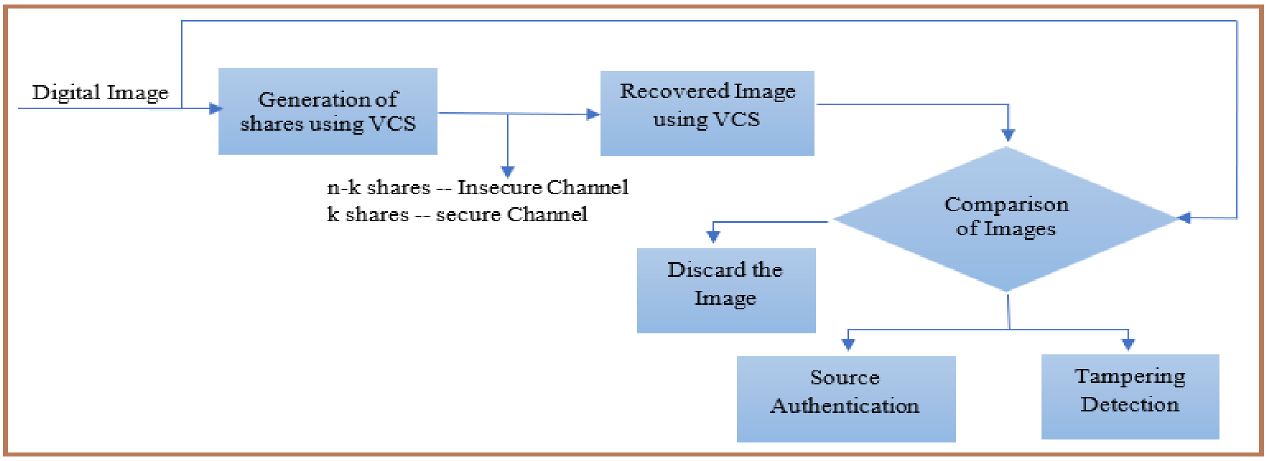
Figure 15: Digital Image Forensics flowchart

A new approach in the form of Visual Cryptography brought forward by Naor and Shamir that requires less computations during secret image reconstruction. In this k-shares out of -n shares of digital image visual cryptography scheme (VCS), k-shares or more are used for transmission over secured channel and n-k shares via insecure channel Figure.16.

Digital Image Forensics is performed either for active and passive detection for forgery in digital image.

Active Digital Image Forensics ensure image authentication, integrity and detection of forgeries, when performed incorporating cheating immune visual cryptography scheme (CIVCS), fortify from cheatingand the malefactor reconstruct the false shares of secret image slicing.

Tackling digital misinformation, a cryptography provenance system partially can work to automate its surfacing and rephrasing to deliver authentic news at the receiver end. Human-centered-computing and security, journalism and cryptography-based literature have been taken into account for content-based and technical mode of misinformation appraisal [44].New approaches to the existing whistleblowing platforms problems through incorporating JavaScript cryptography to lessen the reliance of trust for the hosted servers, anonymous encryption and cover traffic to anonymize the recipient, file size and timing metadata of submissions sent by the whistleblowers are viable options. For India, data availability concerning the domestic use controls of cryptography and imports are not available.



Digital Image
Generation of shares using VCS
Recovered Image using VCS
n-k shares -- Insecure Channel
k shares -- secure Channel
Comparison of Images
Discard the Image
Source Authentication
Tampering Detection

Figure 16: Proposed Active Forensic Model based on Visual Cryptography

Political dissuasions to commit cryptographic research study and practice enforced the need for it in disguise and now stands widely approbated by civil libertarians, transparency activists, journalists and computer scientists for its exigency in extrication of liberal society in digital age.

Being a shared and distributed database for decentralized information sharing, blockchain has opened vistas for distributed ledger technologies use cases in journalism and vivify hope for the industry in abeyance to avail of this secure technology for the sake of intellectual property rights of legit writers. Calibrating the semiotics of news actors in relation to one another and the semantics of covered news in Edward Snowden and WikiLeaks shows the clarity of performances by journalists for their identity creation when the risk factor of genuine news work against the digital news work dynamics were on escalation. Journalistic meta-discourses reveal the identity of journalists who do their professional news-work and those who facilitate mega-leaks by merely digitally operable news contents.

News-safety, a three-dimensional concept enshrines infrastructures, practices and consequences in the era of social media technology necessitate the incorporation of new socio-technological methodology amid high risk to journalists.

2. Scope of Information Security in Journalism

Information security in journalism anticipates many areas of emergence in research. One based upon the instrumentation, application and deployment of infosec tools for journalistic works and another one for its implementation in organizational set-ups, professional and cultural readiness to accept innovative practices trade-offs with traditional one and the rationales of its usage whereas the third one opens new vista of research for interdisciplinary researchers ranging from social science, management and software engineering information technology.

A. InfoSec Instrumentation, application and deployment-based research in journalism

Susan E. McGregor's book Information *Security Essentials. A Guide for Reporters, Editors, and Newsroom Leaders (2021)* has comprehensive coverage of contemporary infosec tools instrumentation, application and deployment in varying newsroom set-ups. Generally, infosec tools are evocative of surveillance activities evasion and protection of sources on job from private and state actors [45]. In the wake of *Journalism after Snowden*, several writers wrote and published research articles including Carl Fridh Kleberg who in his reviewed article discussed about digital evasive solutions of ad hoc surveillance, source protection, safe data communication and its storage and retrieval mechanisms, smartphone security and passcode safety.

UNESCO has published Julie Posetti's *Protecting Journalism Sources in the Digital Age* wherein she suggests encryption tool for digital data information safety for the existing legal framework doesn't enshrine adequate safeguard for investigative journalists who along with their sources always remain at the butt end of state surveillance. In all, surveillance inflicts adrenaline and paranoia to journalists and to their Sources eventually hamstring journalistic practices [46]. Further Mills and Sarikakis [47] suggests encryption Instrumentation in response to such threats. In his study Paul Lashmar found that how journalists have changed their source protection attitudes in the wake of Snowden revelations and suggests encryption tools usage however their efficacy yet to be anatomized. Another study of U.S. national security journalists for their adoption of infosec tools revealed their inconsistencies in using them that further exacerbated the problem. E-mail encryption using PGP is being used by most of them but the whistle blowing software SecureDrop is yet required to have steep learning curve. Whistleblowing software came to limelight after WikiLeaks' classified disclosures and several publications infatuated with the literatures about SecureDrop and GlobaLeaks [48]. The consumer base ecosystem of infosec tools runs a gamut of small to large news media organizations like *The Guardian* and *The New York Times* setting forth new age journalistic practices [49] studied in deep about the whistleblowing platforms' origin links and their business references with the WikiLeaks. The whistleblowing platforms and their history and working radical transparency studied in the light of democratic practices by Luke Heemsbergen [50]. Anglophone news outlets majorly used SecureDrop services for leaks amidst the changing Sourcing resources that extended the boundary work of journalism to hackers as news Source [51]. The culture of cyberlibertarian and cross-border collaborative and secured encrypted communication with Sources are evocative of WikiLeaks' contingency upon leaked papers [52]. State control and the territorial-technology nexus try to influence the anonymity of Sources over trans-border communication through internet. In this perspective also WikiLeaks seems to defend its' ground citing global communication 'freedom of internet' beyond compromise [53]. Usage of encryption methods by the 'intermediaries of change' for cross-border collaboration practices further corroborate the fact that cross-border investigations viz. Europe's *Far Right* and *Panama Papers'* Leak, are the result of entente cordiale of participant nation. Encryption requirements to dodge surveillance has forced to take recourse of dark web by journalists for reporting news of social significance, however the ethical consideration has raised concern over this and warn regular presence can be fatal. African inter-continental Investigative Journalism Networks (IJN) taken as a case of country specific study for usage of encryption tools like Signal and Telegram chatting apps for secure message routing to international counterparts [54]. A study on Nigerian journalists Knowledge, Attitude and Practice (KAP) reveals that they know encryption strategy to safe communication but their practice is limited to strong password protection [55]. Journalists in Zimbabwe knowing their governments' covert surveillance activities have done away with digital mode while investigating serious cases of corruption, chary to leave any metadata trails behind [56]. Amateurish citizen journalists' adoption of infosec tools for anti-surveillance activities revealed abysmally limited knowledge.

B. Individual and organizational behavior Based Infosec research in journalism

In this category such research comes that relate to individual ideas and organizational behavioral and operational need to use infosec. Overall, the rationale and motivation in adopting infosec tools for journalism is researched under this category. In general, what journalists conjure up of listening about infosec, is studied by Susan McGregor and Elizabeth Watkins [57] to come up with their mental model.

They concluded that 'Security by Obscurity' being the collective unconscious for almost all, so until entrusted and assigned with any classified job, infosec oughtn't need be employed. However, authors later profess that such *forma mentis* is fragile and complaisant in nature. In US and France infosec training and expertise rest with solo journalist who eventually handles and maintains covert collusive communication with his confidante/sources [58]. Mental models studied by Lokman Tsui and Francis Lee in Hong Kong came out with three mental propositions namely, 'Security by Obscurity', 'Security by Obfuscation' and 'Security as Opportunity'.

C. Interdisciplinary areas of research in journalism for information security

Another area of research in journalism opening new vistas for information security technocrats about strengthening the online security of existing communication tools viz. satellites, mobile phones and other electronic receiver sets through routing protocols QoS fortification. Sharma *et al* found that there exist many inconsistencies in Optimized Link state routing protocol (OLSR) used for proactive data routing in Mobile ad hoc networks (MANET) for video streaming. The end-users' quality of experience (QoE) in viewing low quality videos due to packet loss in transit over high efficiency video coding H-265/(HEVC) protocols' facilitation for lower bandwidth network supporting smartphones and tablets can be a new avenue of research for social science communication researchers too. Ruan *et al* elaborated the QoE of virtual reality (VR) video streaming on end-users and came out with its' different experiential resonance factors namely System Factors, Context Factors, Human Factors and Psychological Factors responsible for compromised video quality.

V. RECOMMENDATION

1) With progressive technological advancements for infallible fortified privacy, the traditional cryptography based on DES, AES, HASH and Blockchain decentralized and distributed applications seems to succumb to the evolving research in Quantum cryptography that uses less time for big data encryption/decryption *aestriplex* using Quantum Key Distribution (QKD) methodology. To hedge against comprehensible digital attack for database-intrusion utilizing quantum cryptography (QC), a post-QC in the form of Homomorphic Encryption (HE) proposed to be used by many. This utilizes encryption of the cyphertext and their routing over transmission channel without any interference with the plaintext.

Additive to the three steps namely (a) key distribution (b) Encryption and (c) Decryption, the fourth step of (d) Evaluation used in this HE. Its' application can be utilized for media organizations for uninterruptible p2p communication authentication, privacy and integrity corroboration for other businesses like healthcare and private entities heeding over to switch onto this evolving technology.

2) Ali *et al* [59] has proposed a Secure and Privacy-Aware Misinformation Detection as a Service (SPAM-DaS) homomorphic cryptography-based Web-service to proactively detect the misinformation and fake-news.

3) In a beating attempt against HE Yarter *et al* [60] proposed a quantum homomorphic cryptography (QHC) that implements quantum circuits over encrypted qubits. This could be a futuristic privacy implementable tool for information-based industries.

4) Julie Posetti’s UNESCO report 2017 recommendation for media actors and other producers of journalism recommends the obligations resting on the part of the media owners to instrumentalize their investigative reporters and freelancers with sophisticated tools and trainings in order that they could communicate securely with their sources on job. A noble research area emerging related to the enquiry of infosec instrumentation, application and deployment by media owners to meet UNESCO recommendations for journalists’ digital safety.

5) Recommendations for UNESCO member states in Posetti’s report require regional workshops for media plus the civil society to equip them with the necessary training and IT skills to confront issues raised in the study for continuing investigative journalism practice. Such workshops inculcate individual and organizational behavior shifting to adopt InfoSec skills and attention. A noble research area emerges whether the individual and organizational behavior shift achieved after national workshops organized for journalists’ safety and in what frequency the national workshops organized and where? to comply the recommendations in UNESCO 2017 report for journalist safety.

VI. CONCLUSION

In the light of the reviewed and referenced research papers approachable for information security in journalism and related privacy and data-integrity prone fields, it springs out that the more the technologies sophisticate the more the new vistas open showing their deficiency and fallibility to pertinent vulnerabilities. This day when the nascent field of quantum cryptography is emerging and resting as a glimpse in the eyes of top defense governance, the concern for post quantum cryptography is afoot delimiting its application, baying circumspection for probable abusive use to usurp government data by foreign actors. Homomorphic cryptography and quantum homomorphic cryptography too up on the forefront offering infallible data/information privacy and integrity. Still the common people plus the professionals of media and investigative journalism need to bide their time to see the fruitful comeuppance when these technologies govern data transmission over internet for data and information access.

DECLARATION

Funding/ Grants/ Financial Support	No Funding.
Conflicts of Interest/ Competing Interests	No conflicts of interest to the best of our knowledge.
Ethical Approval and Consent to Participate	No, the article does not require ethical approval and consent to participate with evidence.
Availability of Data and Material/ Data Access Statement	Not relevant.
Authors Contributions	I am only the sole author of the article.

REFERENCES

1. S. Arulchelvan, “Internal Threats and Safety of Journalists. A study from India,” *Assault Journal. Build. Knowl. to Prot. Free. Expr.*, 2017.
2. C. Berret, “Newsrooms are making leaking easier–and more secure–than ever,” *Columbia J. Rev.*, 2017.
3. M. Hu, “Cambridge Analytica’s black box,” *Big Data Soc.*, vol. 7, no. 2, p. 2053951720938091, 2020. https://doi.org/10.1177/2053951720938091
4. S. Kirchgaessner, P. Lewis, D. Pegg, S. Cutler, N. Lakhani, and M. Safi, “Revealed: Leak uncovers global abuse of cyber-surveillance weapon,” *Pegasus Proj. Guard.*, 2021.
5. M. R. Patil and C. F. Mulimani, “Pegasus: Transforming Phone Into A Spy,” *Think India J.*, vol. 22, no. 14, pp. 7883–7890, 2019.
6. G. A. Sinha, *With Liberty to Monitor All: How Large-scale US Surveillance is Harming Journalism, Law and American Democracy*. Human Rights Watch, 2014.
7. C. Savage, “Holder tightens rules on getting reporters’ data. New York, NY,” *New York Times*, p. A7, 2013.
8. C. Savage and L. Kaufman, “Phone records of journalists seized by US,” *New York Times*, vol. 13, 2013.
9. A. E. Marimow, “Justice Department’s scrutiny of Fox News reporter James Rosen in leak case draws fire,” *Washington Post*, 2013.
10. M. Crete-Nishihata, J. Oliver, C. Parsons, D. Walker, L. Tsui, and R. Deibert, “The information security cultures of journalism,” *Digit. Journal.*, vol. 8, no. 8, pp. 1068–1091, 2020. https://doi.org/10.1080/21670811.2020.1777882
11. R. Anderson, “Why information security is hard-an economic perspective,” in *Seventeenth Annual Computer Security Applications Conference*, 2001, pp. 358–365.
12. R. Benson, “Book Review: Normative Theories of the Media: Journalism in Democratic Societies.” SAGE Publications Sage UK: London, England, 2011. https://doi.org/10.1080/21670811.2020.1777882
13. C. G. Christians, T. Glasser, D. McQuail, K. Nordenstreng, and R. A. White, *Normative theories of the media: Journalism in democratic societies*. University of Illinois Press, 2010.
14. A. Russell, R. Kunelius, H. Heikkilä, and D. Yagodin, *Journalism and the NSA revelations: Privacy, security and the press*. Bloomsbury Publishing, 2017.
15. V. Bakir, “Journalism and the NSA Revelations: Privacy, Security and the Press.” SAGE Publications Sage UK: London, England, 2017. https://doi.org/10.1177/0267323117730717
16. S. Coll, “5. Source Protection In The Age Of Surveillance,” in *Journalism After Snowden*, Columbia University Press, 2017, pp. 85–96.
17. R. V Ericson and K. D. Haggerty, “The surveillant assemblage,” *Br. J. Sociol.*, vol. 51, no. 4, pp. 605–622, 2000. https://doi.org/10.1080/00071310020015280
18. A. Kwon, D. Lu, and S. Devadas, “{XRD}: Scalable messaging system with cryptographic privacy,” in *17th USENIX Symposium on Networked Systems Design and Implementation (NSDI 20)*, 2020, pp. 759–776.
19. A. E. B. Tomaz, J. C. do Nascimento, and J. N. de Souza, “Blockchain-based whistleblowing service to solve the problem of journalistic conflict of interest,” *Ann. Telecommun.*, vol. 77, no. 1, pp. 101–118, 2022. https://doi.org/10.1007/s12243-021-00860-0
20. J. M. Anderson, “Why we need a new definition of information security,” *Comput. Secur.*, vol. 22, no. 4, pp. 308–313, 2003. https://doi.org/10.1016/S0167-4048(03)00407-3
21. S. E. Chang and C. B. Ho, “Organizational factors to the effectiveness of implementing information security management,” *Ind. Manag. Data Syst.*, 2006.
22. K. J. Knapp, T. E. Marshall, R. K. Rainer, and F. N. Ford, “Information security: management’s effect on culture and policy,” *Inf. Manag. Comput. Secur.*, vol. 14, no. 1, pp. 24–36, 2006. https://doi.org/10.1108/09685220610648355
23. J.-N. Ezingeard and M. Bowen-Schrire, “Triggers of change in information security management practices,” *J. Gen. Manag.*, vol. 32, no. 4, pp. 53–72, 2007. https://doi.org/10.1177/030630700703200404
24. J. Aycock and J. Aycock, “Getting There,” *Spyware and Adware*, pp. 9–27, 2011. https://doi.org/10.1007/978-0-387-77741-2_2
25. B. A. Forouzan, *Data Communications and Networking Global Edition 5e*. McGraw Hill, 2012.
26. S. Baack, “What big data leaks tell us about the future of journalism–and its past,” *Internet Policy Rev.*, vol. 12, no. 23, pp. 9–17, 2016.
27. B. Brevini, “WikiLeaks: Between disclosure and whistle-blowing in digital times,” *Sociol. Compass*, vol. 11, no. 3, p. e12457, 2017. https://doi.org/10.1111/soc4.12457
28. B. Alfter, “Cross-border collaborative journalism: Why journalists and scholars should talk about an emerging method,” *J. Appl. Journal. Media Stud.*, vol. 5, no. 2, pp. 297–311, 2016. https://doi.org/10.1386/ajms.5.2.297_1
29. P. Di Salvo, “Hacking/journalism,” *Limn*, vol. 8, pp. 36–39, 2017.
30. P. Bradshaw, “Chilling Effect: Regional journalists’ source protection and information security practice in the wake of the Snowden and Regulation of Investigatory Powers Act (RIPA) revelations,” *Digit. Journal.*, vol. 5, no. 3, pp. 334–352, 2017. https://doi.org/10.1080/21670811.2016.1251329
31. R. Abu-Salma, M. A. Sasse, J. Bonneau, A. Danilova, A. Naiakshina, and M. Smith, “Obstacles to the adoption of secure communication tools,” in *2017 IEEE Symposium on Security and Privacy (SP)*, 2017, pp. 137–153. https://doi.org/10.1109/SP.2017.65
32. J. Angwin, “7. Digital Security For Journalists,” in *Journalism After Snowden*, Columbia University Press, 2017, pp. 114–129. https://doi.org/10.7312/bell17612-010
33. B. Ataman and B. Çoban, “Counter-surveillance and alternative new media in Turkey,” *Information, Commun. Soc.*, vol. 21, no. 7, pp. 1014–1029, 2018. https://doi.org/10.1080/1369118X.2018.1451908
34. P. Di Salvo, “Securing whistleblowing in the digital age: SecureDrop and the changing Journalistic practices for source protection,” *Digit. Journal.*, vol. 9, no. 4, pp. 443–460, 2021. https://doi.org/10.1080/21670811.2021.1889384
35. J. R. Henrichsen, “Understanding Nascent Newsroom Security and Safety Cultures: The Emergence of the ‘Security Champion,’” *Journal. Pract.*, vol. 16, no. 9, pp. 1829–1848, 2022. https://doi.org/10.1080/17512786.2021.1927802
36. L. Tsui and F. Lee, “How journalists understand the threats and opportunities of new technologies: A study of security mind-sets and its implications for press freedom,” *Journalism*, vol. 22, no. 6, pp. 1317–1339, 2021. https://doi.org/10.1177/1464884919849418
37. P. Di Salvo, “Information security and journalism: Mapping a nascent research field,” *Sociol. Compass*, vol. 16, no. 3, p. e12961, 2022. https://doi.org/10.1111/soc4.12961
38. M. E. Whitman, “In defense of the realm: understanding the threats to information security,” *Int. J. Inf. Manage.*, vol. 24, no. 1, pp. 43–57, 2004. https://doi.org/10.1016/j.ijinfomgt.2003.12.003
39. J. M. Hagen, E. Albrechtsen, and J. Hovden, “Implementation and effectiveness of organizational information security measures,” *Inf. Manag. Comput. Secur.*, 2008.
40. S. Carlo and A. Kamphuis, “Information security for journalists,” *Cent. Investig. Journal. London*, 2014.
41. J. Posetti, *Protecting journalism sources in the digital age*. Unesco Publishing, 2017.
42. C. F. Kleberg, “The death of source protection? Protecting journalists’ source in a post-Snowden age,” 2015.
43. P. Lashmar, “No more sources? The impact of Snowden’s revelations on journalists and their confidential sources,” *Journal. Pract.*, vol. 11, no. 6, pp. 665–688, 2017. https://doi.org/10.1080/17512786.2016.1179587
44. E. Sidnam-Mauch *et al.*, “Usable Cryptographic Provenance: A Proactive Complement to Fact-Checking for Mitigating Misinformation,” in *Proceedings of the International AAAI Conference on Weblogs and Social Media*, 2022, vol. 16, no. 2022.

45. D. Glowacka, K. Siemaszko, J. Smtek, and Z. Warso, “Protecting journalistic sources against contemporary means of surveillance,” *North. Light. Film Media Stud. Yearb.*, vol. 16, no. 1, pp. 97–111, 2018. https://doi.org/10.1386/nl.16.1.97_1
46. A. Mills, “Now you see me–now you don’t: Journalists’ experiences with surveillance,” *Journal. Pract.*, vol. 13, no. 6, pp. 690–707, 2019. https://doi.org/10.1080/17512786.2018.1555006
47. A. Mills and K. Sarikakis, “Reluctant activists? The impact of legislative and structural attempts of surveillance on investigative journalism,” *Big Data Soc.*, vol. 3, no. 2, p. 2053951716669381, 2016. https://doi.org/10.1177/2053951716669381
48. P. Di Salvo and E. Leaks, *Digital Whistleblowing Platforms in Journalism*. Springer, 2020. https://doi.org/10.1007/978-3-030-38505-7
49. A. Greenberg, *This machine kills secrets: Julian Assange, the Cypherpunks, and their fight to empower whistleblowers*. Penguin, 2013.
50. L. Heemsbergen, *Radical transparency and digital democracy: Wikileaks and beyond*. Emerald Group Publishing, 2021. https://doi.org/10.1108/9781800437623
51. P. Di Salvo and C. Porlezza, “Hybrid professionalism in journalism: Opportunities and risks of hacker sources,” *Stud. Commun. Sci.*, vol. 20, no. 2, pp. 243–254, 2020. https://doi.org/10.24434/j.scoms.2020.02.007
52. L. Lynch, “‘We’re Going to Crack the World Open’: Wikileaks and the future of investigative reporting,” in *The Future of Journalism*, Routledge, 2013, pp. 243–252.
53. R. Zajácz, “WikiLeaks and the problem of anonymity: A network control perspective,” *Media, Cult. Soc.*, vol. 35, no. 4, pp. 489–505, 2013. https://doi.org/10.1177/0163443713483793
54. R. Meyer, “‘Wearing a Bullet-Proof Vest’: Social Media Use in Journalism Production Within African–Intercontinental Investigative Networks,” *African Journal. Stud.*, vol. 40, no. 3, pp. 89–106, 2019. https://doi.org/10.1080/23743670.2020.1730215
55. O. A. Suraj and O. Olaleye, “Digital Safety among Nigerian Journalists,” *Assault Journal.*, p. 329.
56. A. Munoriyarwa, “When watchdogs fight back: resisting state surveillance in everyday investigative reporting practices among Zimbabwean journalists,” *J. East. African Stud.*, vol. 15, no. 3, pp. 421–441, 2021. https://doi.org/10.1080/17531055.2021.1949119
57. S. E. McGregor and E. A. Watkins, “‘Security by Obscurity’: Journalists’ Mental Models of Information Security,” in *International Symposium on Online Journalism*, 2016, vol. 6, no. 1, pp. 33–49.
58. E. A. Watkins, M. N. Al-Ameen, F. Roesner, K. Caine, and S. McGregor, “Creative and set in their ways: Challenges of security sensemaking in newsrooms,” in *7th USENIX Workshop on Free and Open Communications on the Internet (FOCI 17)*, 2017. https://doi.org/10.36227/techrxiv.19351679.v1
59. H. Ali *et al.*, “SPAM-DaS: Secure and privacy-aware misinformation detection as a service.” TechRxiv, 2022.
60. M. Yarter, G. Uehara, and A. Spanias, “Implementation and Analysis of Quantum Homomorphic Encryption,” in *2022 13th International Conference on Information, Intelligence, Systems & Applications (IISA)*, 2022, pp. 1–5. https://doi.org/10.1109/IISA56318.2022.9904399

AUTHORS PROFILE

Rajeev Ranjan Sahay, The author pursue his Ph.D in Mass Communication & Journalism from USJMC, Uttaranchal University, Dehradun, Uttarakhand, India under session 2023-25. Earned his MA in Mass Communication and Journalism from Banaras Hindu University, Varanasi in the year 2010-12. Concurrently, cracked UGC-NET (Mass Communication and Journalism), June 2012 examination. From 2017 to 2018, has been in the helm of the email administrative communication of CM Secretariat, Bihar. Also has the expertise of cracking Prasar Bharti’s ‘Anchor-cum-Correspondent Grade II’ examination for which the audition test held in Nov. 5, 2019 at Doordarshan News, India, New Delhi.

APPENDIX

TABLES USED

FIGURES USED

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of the Lattice Science Publication (LSP)/ journal and/or the editor(s). The Lattice Science Publication (LSP) and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.