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 to synthesize existing practices in this field. Initially, existing research article databases and search engines are utilised to download or retrieve the abstracts of relevant scientific articles, which are then used for systematic and rigorous citation and summarisation works. Contingent upon them, their analysis and synthesis are employed to arrive at the findings. Research papers collated to write this review paper highlighted the vital issues related to the inadequacies of investigative journalists' safety practices, even after the UNESCO guidelines of 2017 and 2022, which emphasised the urgent need for member States to address journalists' needs.*

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

I. INTRODUCTION

The freedom enjoyed by citizens in a country is the proper measure of 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 coercion of the duty of journalists by any state/private actors is considered a threat to them. Today, journalists often underperform due to threats, which affects the public's need for accurate information. [1]. In recent times, digital attacks on journalists and the subsequent 'missing in action' cases have raised concerns about gratuitous surveillance and necessitated the implementation of information security in journalism, utilising encryption technology. Cryptography is an information security practice that converts plain text information into encrypted cyphertext before online transmission over the internet. Encryption is the method of practising cryptography on soft plain documents. Today, no academic institution or university that teaches journalism as a vocational core curriculum has arrangements to impart information security training, either in a project work format or as a major, minor elective, or specialisation. In this information technology society, it seems high time to include 'information security' in journalism course curricula. Edward Snowden's Revelation of the ramifications of mass covert surveillance of journalists has raised concerns among working journalists and prompted them to reconsider information security practices in journalistic work. Coleman opine that in the wake of Snowden revelations, usage of infosec blockchain software applications like SecureDrop and Signal has increased since then by journalists [2]. Earlier, due to a lack of concern for the gravity of covert digital surveillance, encryption for information security was seldom used in journalism. Coverage of encryption-related Leads increased after Snowden whistleblowing. The Cambridge Analytica Case of data manipulation and weaponization [3] Snowden further aggravated concerns about information security and encryption in journalism. Recently, the Pegasus Spyware intrusion sting by Israeli software technocrats and foreign hackers has turned the heads of newsrooms and journalists, making them aware and vigilant about their electronic gadgets being used for journalism. [4], [5]. In recent years, Journalist-Source communications have been put in the limelight due to increased government surveillance activities. [6] and legal frame-ups against sensitive Sources in Britain and the US, as per Marimow, Savage and Kaufman [7]–[9]. The surveillance invisibility connoted a "Black Box Metaphor," whose internal mechanism and threat level obscurity cannot be inferred due to dissimulation, inner elusiveness, and its multiform nature. European ICIJ investigative journalists have vindicated the importance of information security education and training. Overall, a seamless umbrella approach to the study of digital threats to journalism is *erenata*. Surveillance is among the most rampant 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". English-speaking countries' media outlets are evangelically using SecureDrop as a whistleblowing platform software provider to keep their sources anonymous. The use of SecureDrop in countries where journalism hasn't yet developed still needs to be researched. For Journalists working in a "Free Press System" and in Authoritarian States, there is a need to research 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

© The Authors. Published by Lattice Science Publication (LSP). This is an open-access article under the CC-BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

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 an understanding of the amplitudes and potential differences. Amidst the persisting threats to the Source-cum-confidant privacy and digital-bashing of press freedom, journalists need to create the skill to ensconce themselves in this fluid and fragmented security culture to fill the gaps. There is a need for a uniform information security culture for journalists. [10]. Management of InfoSec is an abysmally complex and filibustered problem, and hammering out solutions is likely to be achieved with acumen partially. At the same time, many ex parte and blinkered, simplistic technical approaches are bound to founder. These awful backdrops have necessitated, on the part of engineers, economists, lawyers, and policymakers, to congregate and come under a brolly to try to forge common ground. Network hardware and software externalities, the 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 blocks that inhibit InfoSec infallibility. [11].

The Linux OS is an open-source software built on a multitasking, multiuser kernel, offering web application security compared to Windows. No system can be foolproof; however, enabling adequate security options can help filter web application communication and protect information exchanged over the internet. The Amnesic Incognito Live System (Tails OS) is a Linux-based Debian distribution that offers anonymity and a surveillance-proof browser, Tor, for incognito web surfing and data exchange. Tor Web Browser is a complementary software that runs over Tails. Built on top of the Linux kernel, it supports the Android OS. TrueCrypt, the data encryption tool initially embedded and available for Windows, Mac, and Linux, has been discontinued. VeraCrypt is offering services now instead. PGP Email Encryption is an integrated web service that provides 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 the Freedom of the Press Foundation for confidential communication between Journalists and their Sources. Signal Messenger App is a multi-platform software developed by Signal Foundation for instant voice and video encryption and transmission. This review paper contributes to the readers by apprising them of the persisting limitations against gratuitous surveillance and the state's ignorance of freedom of expression, as evidenced by prolonged investigations aimed at targeting journalists. Section 1 provides a concise introduction to information security in journalism, including the procedure for accessing relevant data, the number of research papers and books/articles referenced, and their general findings. Section 2 discusses the importance 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 organisational behaviour-based research, are suggested for future researchers within the scope of the study in Section 5. The 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 study's methodology is presented in detail. The primary objective of this study is to examine the significance, applications, and limitations of information security in journalism. Based on 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 used in the Search Engines of Scopus, Google Scholar, IEEE Explore, ScienceDirect, and Web of Science for obtaining and identifying 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 the above databases, the following process is to select which articles need to be included and excluded from the study. The exclusion criteria are: articles with no full text, articles that repeat the same methodology, thesis, and documentation of graduation and post-graduation studies. After selecting the articles, the number of articles included in the study is illustrated in Table 2. The year-wise publications are detailed and presented clearly. Additionally, we have mapped the number of articles corresponding to their publication year through a colour-band-coded format visualisation. Colour bands in beige, sky, and light pink represent the duo collective multi-rows, namely “No. of Articles taken” and “Year of publications”, correlating the data for their respective columns.

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), it has sought to maintain the economic and governmental balance of power within the state. [12], [13]. This watchdog role has contributed to the government's accountability in enforcing action to ponder, plan, and purge, addressing the persistent inconsistencies that hinder the state's inclusive development. Hence, work towards an informed, infrastructure-driven, and inclusive public that exhibits its power through righteous voting discernment to elect accountable representatives to the governing chair. *Laissez-faire* working environment with autonomy to communicate with their confidant Sources to bring to the public gaze a mirror image of political developments, is crucial, as Budarick and Waisbord avers, the socio-political independence of the press is essential 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 revelation by former NSA contractor Edward Snowden of covert mass surveillance, a groundswell of unrest has arisen about being tracked at work and being held incommunicado. Moreover, trails of metadata from internet surfing history can be used to track journalists and their confidants/sources without a formal subpoena against them by the state. Hence, "to defeat surveillance and prosecutorial intrusions and to strengthen the rights of journalists before the courts … journalists must 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 the 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 the government legitimises mass surveillance, it becomes imperative for journalists to commit to protecting the privacy of themselves and their sources. Infringements on journalists' privacy have been reported in recent years, including data interception, interception, and unauthorised retrieval, which have had a chilling effect on such threats. This has led sources to be wary of cooperating with their journalists. The Pew Research Centre disclosed that the decreasing resources available in newsrooms and journalists' sporadic use of Infosec tools to evade interception and surveillance have contributed to a sense of complacency. Most journalists, despite being adept at using information security tools such as TLS and Signal, often overlook the fact that their metadata trails on the internet, including browsing time, workstation IDs, location, and communication data size, can be misused by malefactors to serve 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, as shown in Figure 1 below, comprises users, mix-chain servers, and mailbox servers. Each user chooses a discrete random chain of servers, which includes at least one honest server, with an overwhelming probability that their shuffled messages will be routed over networked servers that eventually drop messages into users' mailboxes. Due to shuffling messages over mix-chain servers, users' metadata remains unidentified.

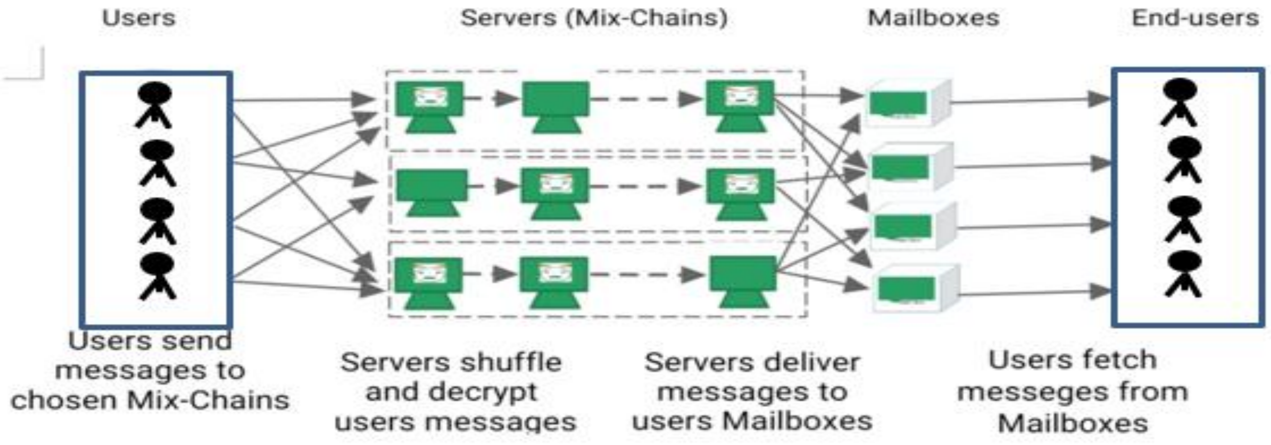
Users
Servers (Mix-Chains)
Mailboxes
End-users
Users send messages to chosen Mix-Chains
Servers shuffle and decrypt users messages
Servers deliver messages to users Mailboxes
Users fetch messeges from Mailboxes

Figure 1: Overview of XRD Operation

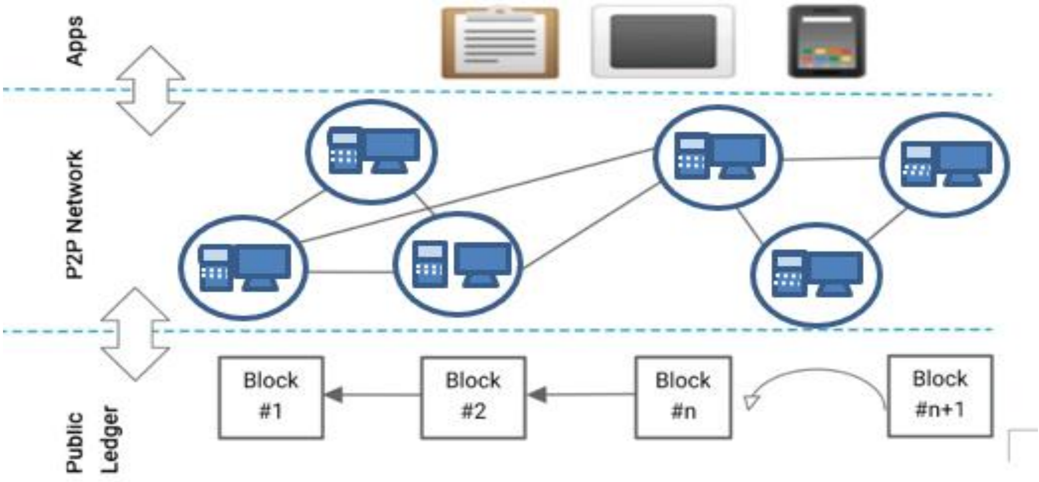

Figure 2: Structure of Blockchain

Resolving conflict of interests arising due to the 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 the significance of Information Security in Journalism

Author (s) & year	Findings
R. Anderson [11]	Network hardware and software externalities, the 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 blocks 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 firm's prime requirement is to have an umbrella information security and practices management.
K. J. Knapp *et al* [22]	Supraordinate management camaraderie and support are very crucial for an information security program and policy.
J.-N. Ezingeard *et al* [23]	Superior management acumen, bolstered by evangelical support, facilitates the timely upgrade of information security systems.
J. Aycock *et al* [24]	This is the system's 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, which are a must-read for gaining 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 the dialectical pros and cons of the 'Leaking to Public' strategy adopted by Assange.
B. Alfter [28]	Cross-border Journalism is the demand of the hour for beats related to transboundary international concerns, including human rights, prescribing a methodology for this.
P. Di Salvo [29]	In this Information era, information protection is paramount for a journalist to sustain themselves in a competitive environment.
P. Bradshaw [30]	Due to a technological and legal knowledge gap, journalistic practices suffer significantly. Improvised training should be provided to alleviate this insecurity.
R. Abu-Salma *et al* [31]	Due to a lack of sketching users' mental models and the inefficient ergonomics of security tools in addressing their contextual needs.
J. Angwin [32]	Cub-reporters need to be familiar with the usage of InfoSec tools.

B. Ataman [33]	This article focuses on the state's oppressive policy adopted by Turkey for the maintenance of state hegemony over the media.
M. Crete-Nishihata *et al* [10]	There is a need for a uniform information security culture among journalists.
P. Di Salvo [34]	SecureDrop usage in countries where journalism hasn't yet developed still needs to be researched.
P. Di Salvo [34]	European ICIJ investigative journalists opined that Information Security education & training are critical.
J. R. Henrichsen [35]	With the increasing institutionalisation of SecureDrop in newsrooms, homogenised journalistic practices will emerge on their own.
L. Tsui *et al* [36]	This article presents information security (InfoSec) practices by journalists working in either China or Hong Kong. However, please provide a ballpark estimate of the fate of journalistic practices in other parts of the world that lack adequate InfoSec Tools.
P. Di Salvo [37]	InfoSec tools are being connoted for "Tools of Press Freedom".

Along with the significance of information security, Table 4 discusses various studies on information security policy, awareness, and training. The findings of each study are summarised in Table 4.

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

Author (s) & year	Findings
M. E. Whitman [38]	Amidst the disruptive airing of threats and breaches to information security, a blitzkrieg in the press, there is a vital need to plug the loophole through awareness, education, and policy.
J. M. Hagen *et al* [39]	Non-technical measures of information security awareness creation were found to be a stronger approach in comparison to the techno-administrative ones.
S. Carlo *et al* [40]	This is a high-level, detailed training kit for all practising 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 rise, posing security threats. The usage of Artificial Intelligence in Journalism for content robotisation is a recent application software advancement that utilises well-structured data feeds to generate automated, mechanised, and full-proof content for publication, independent of human literature. For many, this has facilitated the profession's drudgery.

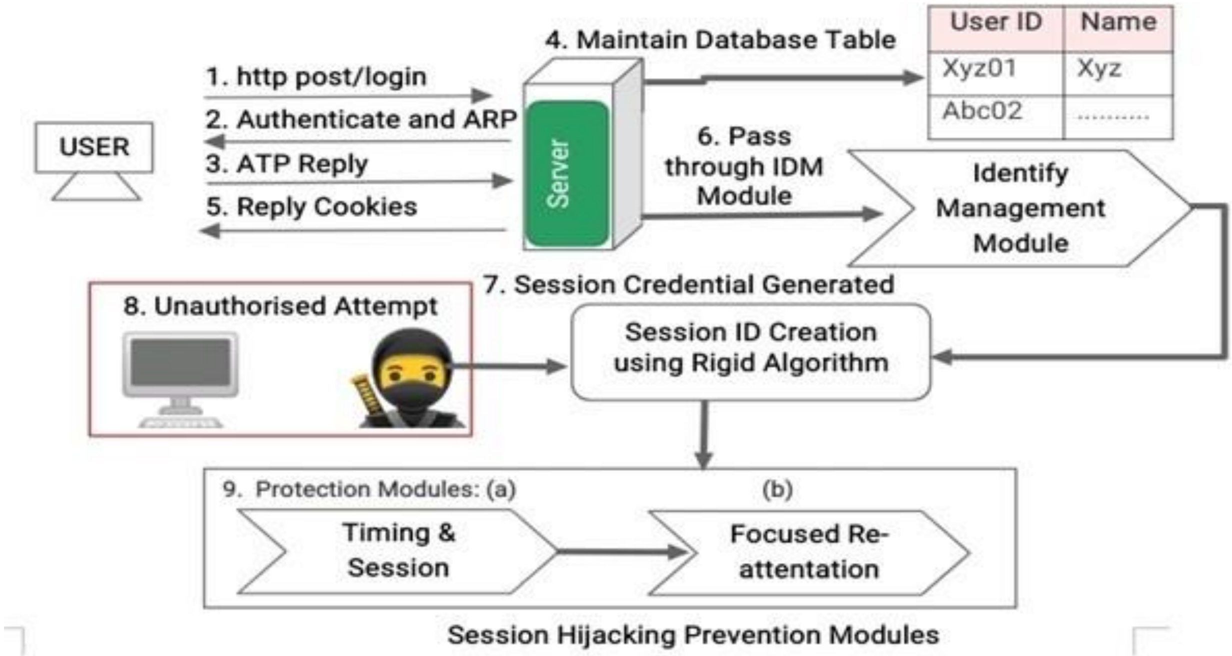
USER
1. http post/login
2. Authenticate and ARP
3. ATP Reply
5. Reply Cookies
Server
4. Maintain Database Table
User ID
Name
Xyz01
Xyz
Abc02
....
6. Pass through IDM Module
Identify Management Module
7. Session Credential Generated
8. Unauthorised Attempt
Session ID Creation using Rigid Algorithm
9.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

Figure 3: General Architecture of session hijacking

Web application, Mobile and Application Programming Interface (API) related security breach vulnerabilities are the prime areas under InfoSec remediation for data-based journalism. Toolkits, such as 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 a web application security breach perpetrated using tools such as T-Sight, TTY Watcher, Hamster, Ferret, Wire Shark, Ethereal, Juggernaut, and Hunt, among others. This breach can be averted through the creation of session IDs using a strong, long, random alphanumeric character algorithm, implementing time-out sessions, and forcing re-authentication.

B. Vulnerability Management

Risk reduction is the prime target of the Information Security Management System. The relationship among asset, threat, and vulnerability, as shown in Figure 4 below, guides the framing of probable targets of evaluation (TOE) as shown in Figure 5, infra. ISO/IEC 19791 is the standard for operational 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 *infra*. Together, the InfoSec security functional requirements, along with the InfoSec security assurance requirements, confer protection from ISMS vulnerabilities and threats. The proposed framework for the ISMS, as outlined by the CC, is illustrated in Figure 6.

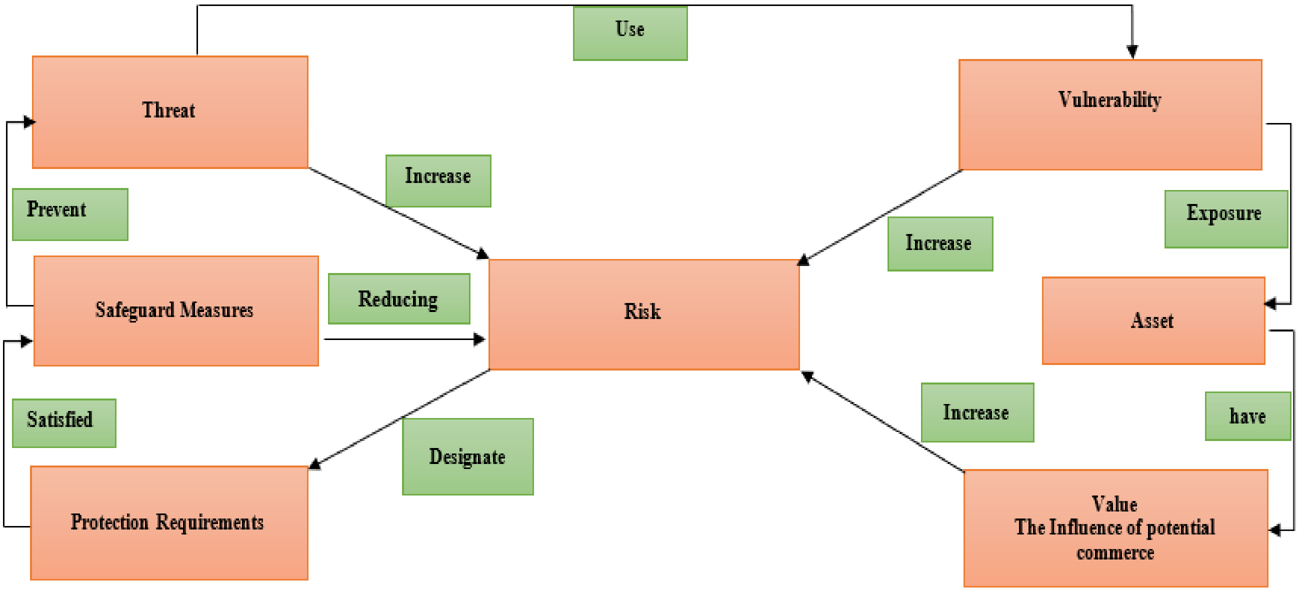

Figure 4: ISMS risk component flowchart and relationship (ISO/IEC TR 13335-1)

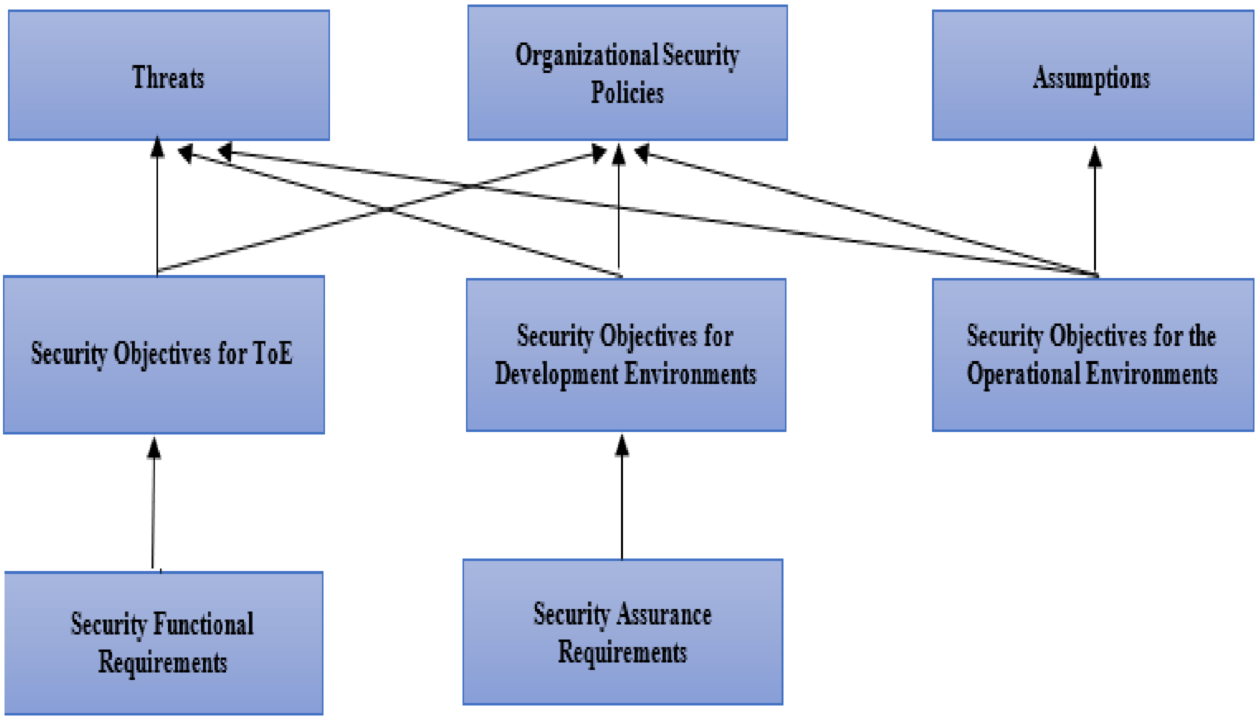
Threats
Organizational Security Policies
Assumptions
Security Objectives for ToE
Security Objectives for Development Environments
Security Objectives for the Operational Environments
Security Functional Requirements
Security Assurance Requirements

Figure 5: Relationship between security objectives and requirements

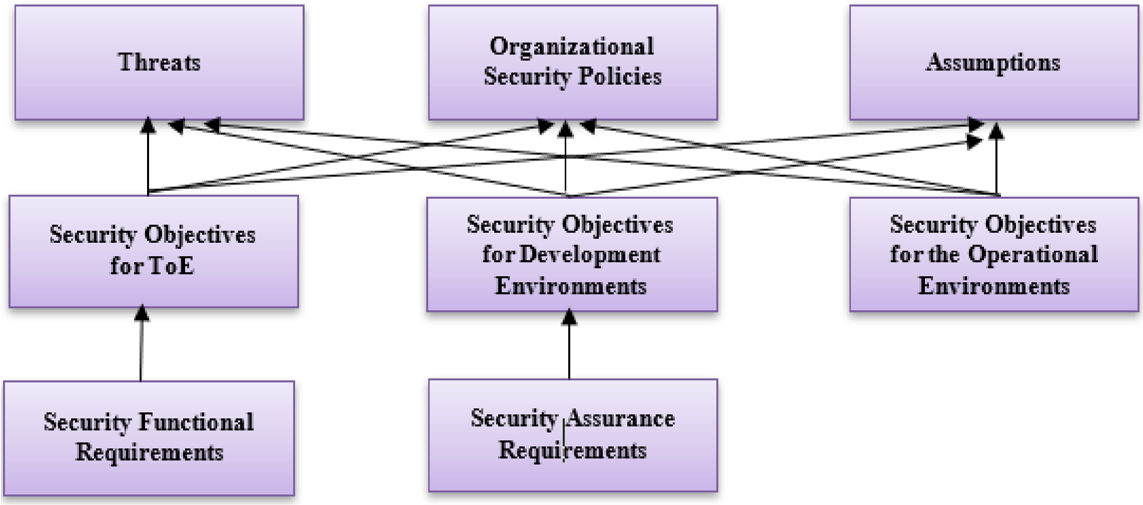
Threats
Organizational Security Policies
Assumptions
Security Objectives for ToE
Security Objectives for Development Environments
Security Objectives for the Operational Environments
Security Functional Requirements
Security Assurance Requirements

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

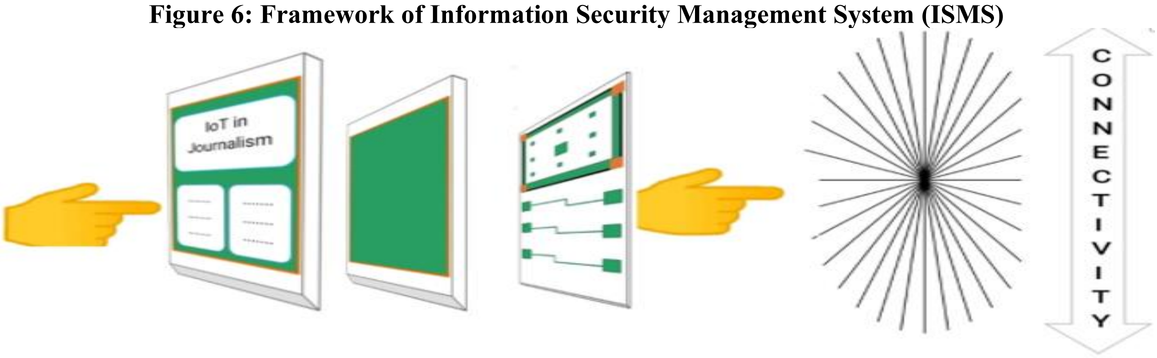

Figure 7: IoT-based Online News Media

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 use a large pool of interconnected and distributed computing resources that can be employed or released with minimal effort by 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).

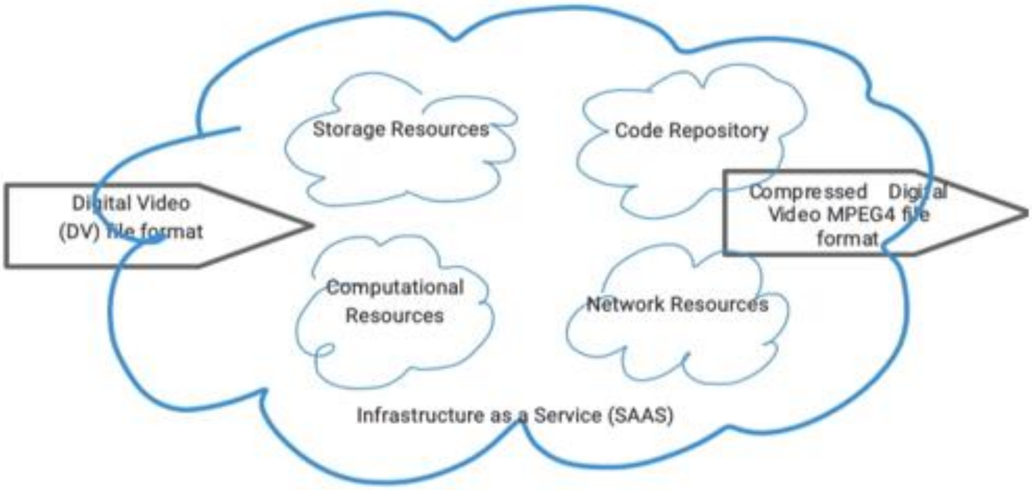
Storage Resources
Code Repository
Digital Video (DV) file format
Compressed Digital Video MPEG4 file format
Computational Resources
Network Resources
Infrastructure as a Service (SAAS)

Figure 8: Cloud Computing Platform

The Internet of Things (IoT) refers to the connectivity of physical things with the internet, enabling 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.

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*.

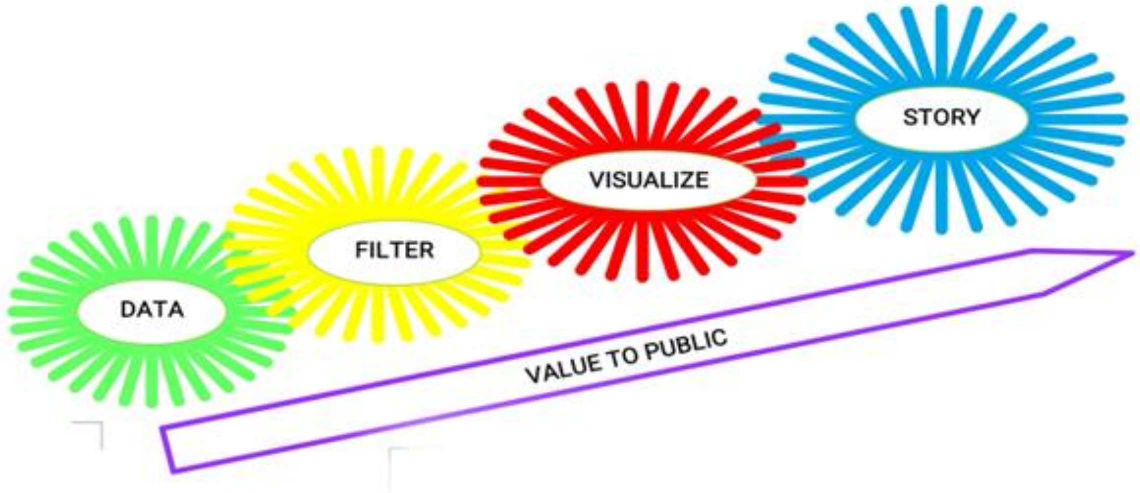

Figure 9: The process chart for visualizing data-mining

Data-driven journalism incorporates the visualisation of data mining over the cloud by exploring, displaying, and expressing data meanings through visual communication that transcends the barriers between information and communication, as shown in the Figure.9 Another cloud application is secure mobile payments over the cloud, a run-of-the-mill issue nowadays because the Europay MasterCard Visa (EMV) application provider's role has been substituted with trusted cloud payment applications stored in the cloud. Compelled disclosure to the government, data security, and disclosure of breaches, as well as data availability and data localisation, are among the key privacy issues in cloud computing, alongside client-server security, location and control of data, and 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 cloud computing, securing data on the cloud, installing and maintaining firewalls, encrypting data, and addressing backup and recovery issues are among the key 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 in information security across different fields include information confidentiality, integrity, availability, and non-repudiation. Algorithms

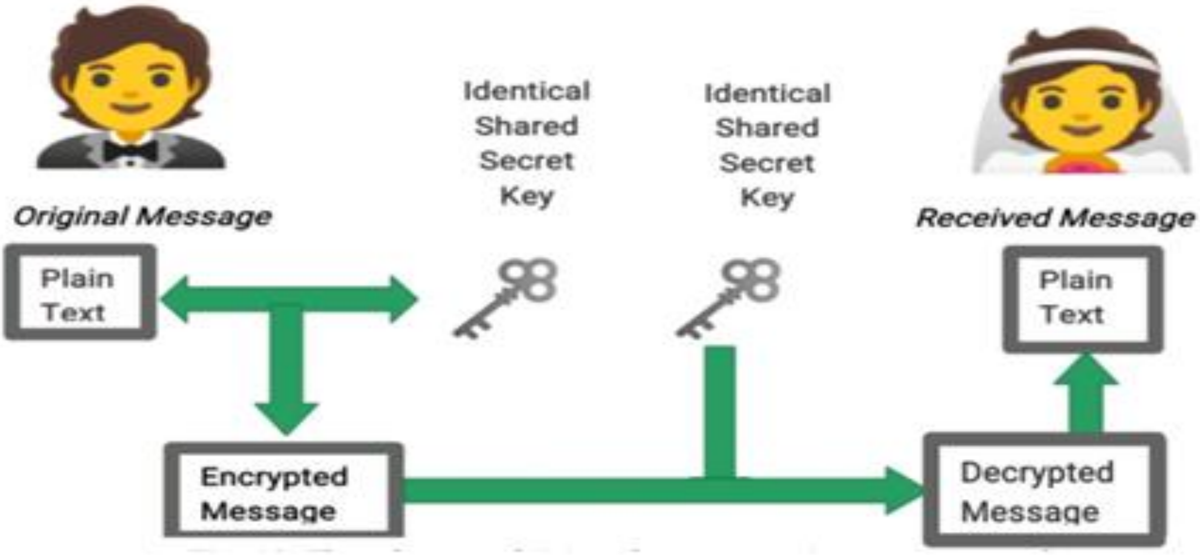

Figure 10: Flowchart explaining the symmetric encryption schemes.

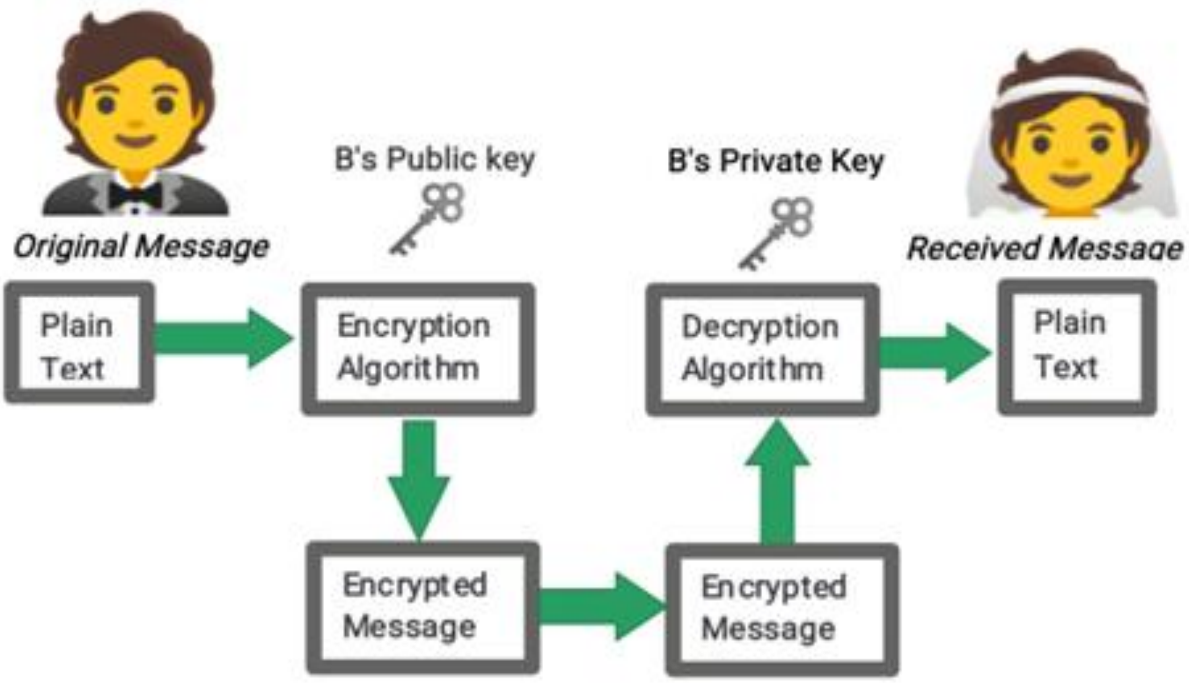

Figure 11: Flowchart explaining the asymmetric encryption schemes.

To implement cryptography, the following standards are commonly used: the Data Encryption Standard (DES), the Advanced Encryption Standard (AES), Identity-Based Encryption (IBE), and the Rivest-Shamir-Adleman Algorithm (RSA). The asymmetric encryption method in Figure 11 requires a pair of keys, a public key and a private key, for each party involved in online communication. In contrast, symmetric key cryptography in Figure 10 uses a single key for exchange between parties for communication. Quantum computing is gaining momentum with every passing day, rendering traditional asymmetric key cryptography, as well as symmetric key cryptography to a moderate extent, obsolete.

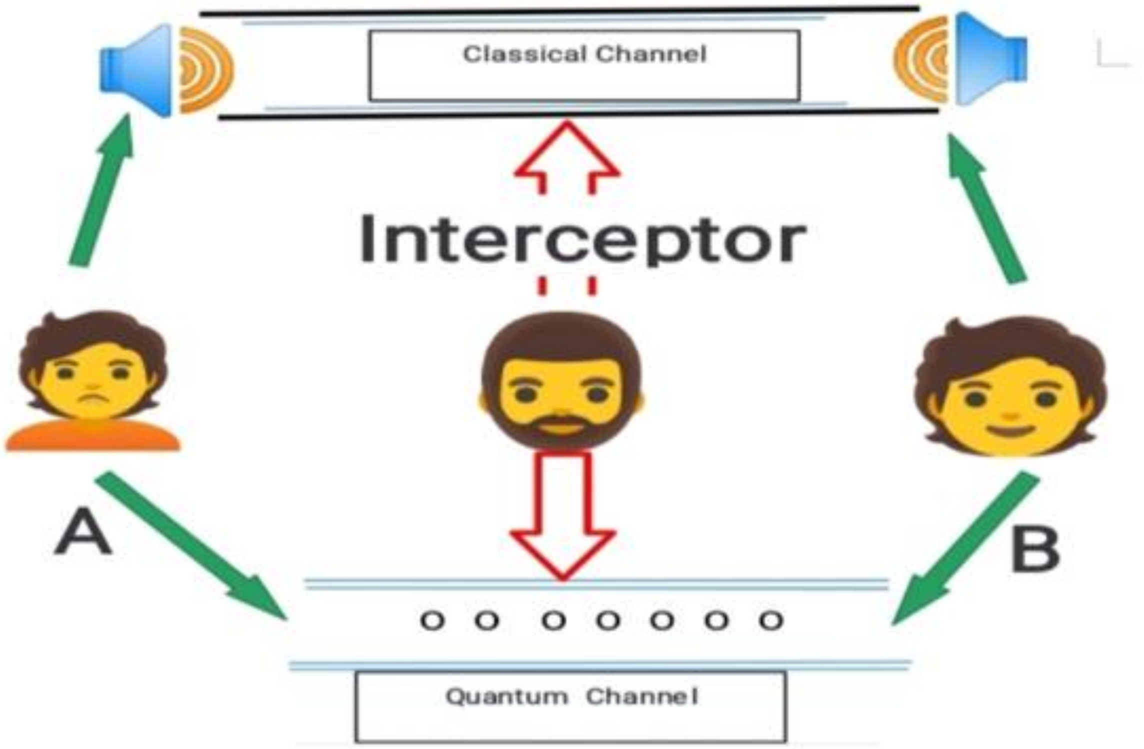

Figure 12: QKD Model for BB84 protocol

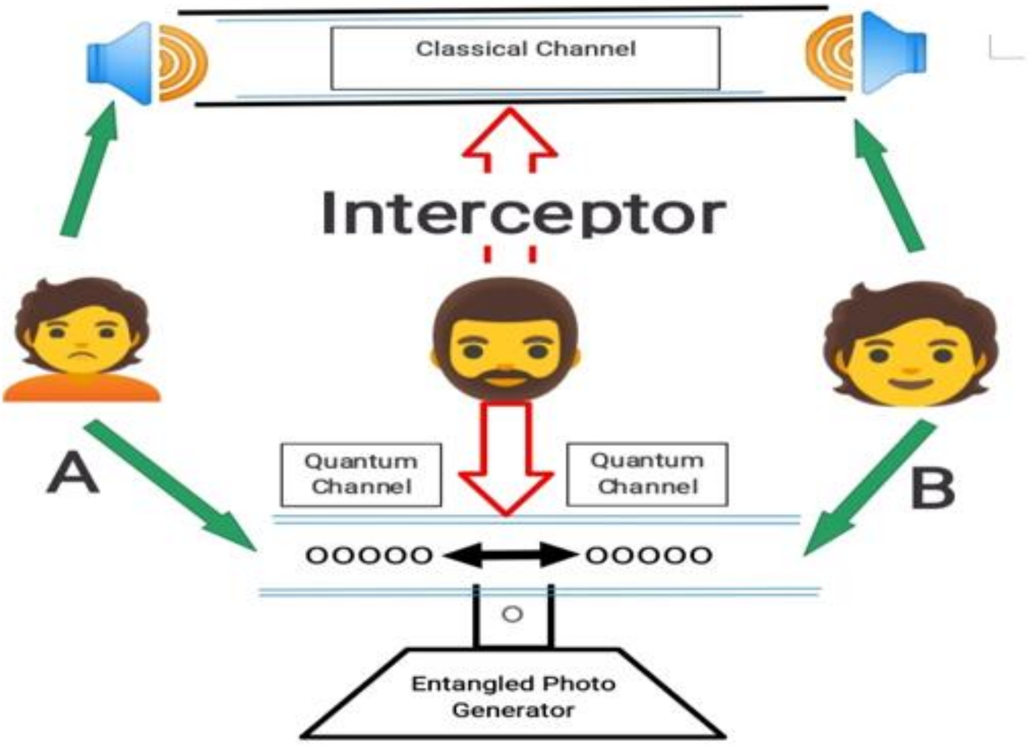

Figure 13: QED Model for Eckert's protocol

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

E. Infrastructure based Security

In the context of infrastructure-based security in journalism, it encompasses device-based security, media-based security, and infrastructure system hardening. Device-based security includes Firewalls, Routers, Switches, Modems, remote access service (RAS), Telecom/Private Branch eXchange (PBX), VPN, IDS, Network Monitoring/Diagnostic, Workstations, Servers and Mobile devices, *etc cetera*

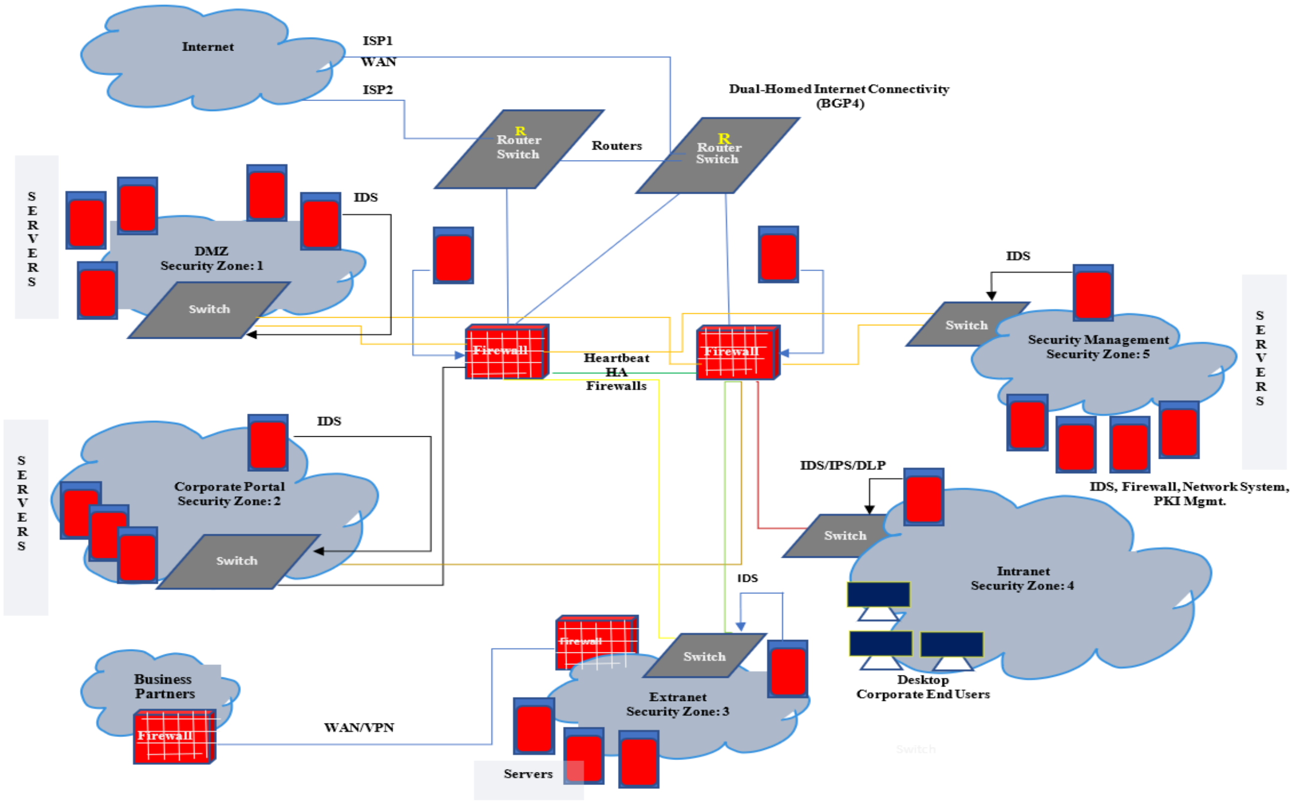

Figure 14: Secure Extranet and Private Cloud

Media-based security encompasses various technologies, including Coax, UTP/STP, Fibre Optic, Removable Media, Magnetic Tape, CDs, DVDs, hard drives, Diskettes, Flashcards, Smartcards, and others. 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 systematically and holistically.

To tackle such socio-technological issues, newspaper publishers and IT companies have collaboratively made headway in incorporating new tools and methodologies into journalistic practices through the use of fact-checking software. The International Consortium of Investigative Journalists (ICIJ), in collaboration with the École Polytechnique Fédérale de Lausanne (EPFL), has developed a Datashare platform that enables reporters worldwide to navigate and share documents required for their 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 needed. The development of an adequate enterprise information infrastructure, IT infrastructure management, and business and IT alignment are key management activities necessary to have a significant impact on enhancing the quality of information security management.

D. Incidence Response based Security

Incidence response-based security is an enhanced management skill that emphasises early and earnest monitoring and detection of comprehensible breaches in computer local and network security, and their timely response to plug and clog the critical loopholes. With the growing interest in cyberspace security and the inherent development that has grown from undercover hacking activities to 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 Butler's Firesheep, an add-on to the Firefox web browser, exposed unencrypted data transmission facilities for end-users to monitor data traffic over public Wi-Fi, prompting social media platforms (Facebook and Twitter) to switch to an enhanced https-based login for their app users. Photobucket, an online photo-sharing platform, has a vulnerability that exposes users' private photo files, relying on 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 incident-response strategy, can infer and learn from familiar end-users' behaviour to fortify and bolster security accessibility. The 2012 LinkedIn user account password leak by the Russian-language forum prompted the company to take action, allowing users to reconfigure their passwords. Similarly, eHarmony also bolstered its platform's security by utilising hashing and encryption techniques, as well as implementing 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. The Indian Computer Emergency Response Team (CERT) issued an advisory on January 20, 2021, against rising data-security breach activities as a proactive measure to curb these online vulnerabilities, a hardliner against malefactors operating with impunity. Raju and Geethakumari studied the security and intrusion detection-handling process of cloud computing. They proposed an intrusion incident detection algorithm to collate intrusion data that can be legally used in 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 practising digital journalism and to provide a carapace to their sources have been undertaken by many, namely, a report in UNESCO for their International Survey of Journalists, Posetti [41] reporting about how to protect journalism sources in a 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, code-breaker William Friedman, deliberately leaked encryption in their devices in 1950 to funnel vital information to Washington and other allies, allowing them to intercept and read messages. This goes by the codename appellations 'Thesaurus' or 'Rubicon', which was one of the sensational security breaches since The 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'.

The digital transformation of Investigative Journalism has opened vistas for encrypted, manipulable, tampered-with, and decentralised information, which has mandated the fabrication and adoption of sophisticated software and mindsets to make headway against disruptive tendencies. Data Journalism sites, namely Vox, FiveThirtyEight, and Quartz, and their inclusion in journalism education show how Words and Statements, Digital Photos, and Videos are abstracted and archived as data in spreadsheets. Image forgery detection, which involves detecting image duplication, is performed through online services such as *Google Image* and *TinEye* for social media content verification. Metadata for Social Media Forensics is not adequate and utilises services from Imageforensic or Reveal, as well as on-premises tools such as Ghiro, Jpegsnoop, and *Phoenix*.

Edward Snowden's revelations have sparked a frisson among investigative journalists to adopt the new normal through ‘Going back to the Analog’ and farming out and outsourcing services to information clearinghouses, such as the International Consortium of Investigative Journalists (ICIJ). Currently, Digital Image Forensics incorporates digital signatures and Digital Image Watermarking to investigate image forgery, providing image authentication and unquestionable image integrity that can be applied during image capture and storage for image ownership authentication (Figure 15).

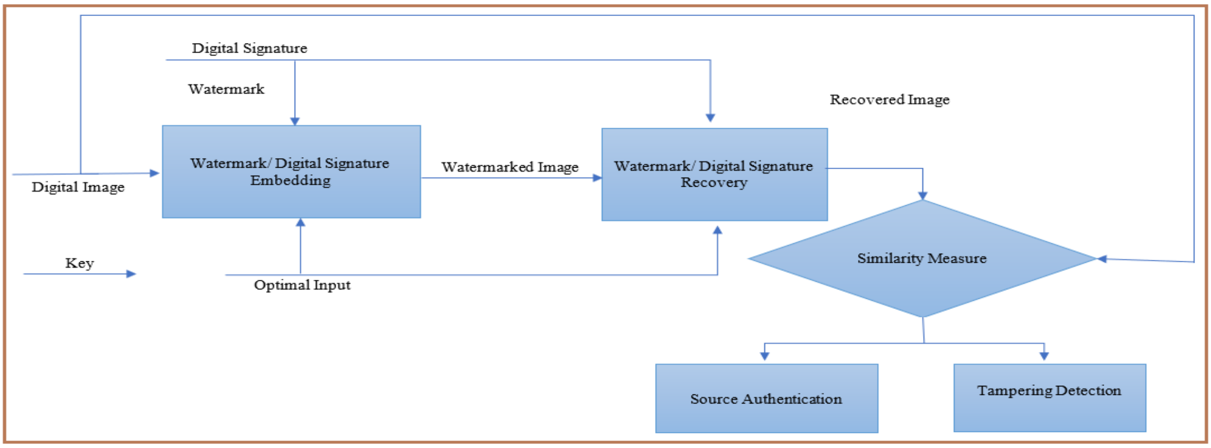

Figure 15: Digital Image Forensics flowchart

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 a secure channel, and n-k shares via an insecure channel (Figure 16).

Digital Image Forensics is performed for both active and passive detection of forgery in digital images.

Active Digital Image Forensics ensures image authentication, integrity, and detection of forgeries when performed by incorporating a cheating-immune visual cryptography scheme (CIVCS), thereby fortifying against cheating and preventing the malefactor from reconstructing the false shares of a secret image.

Tackling digital misinformation, a cryptography-provenance system can partially automate the surfacing and rephrasing of authentic news to deliver it to the receiver. Human-centred computing and security, as well as journalism and cryptography-based literature, have been taken into account for content-based and technical modes of misinformation appraisal. [44] New approaches to addressing the existing problems with whistleblowing platforms can be explored through incorporating JavaScript cryptography to reduce the reliance on trust for hosted servers. Anonymous encryption and cover traffic can be used to anonymise the recipient, while also anonymising file size and timing metadata of submissions sent by whistleblowers. For India, data on domestic use controls of cryptography and imports is not available.

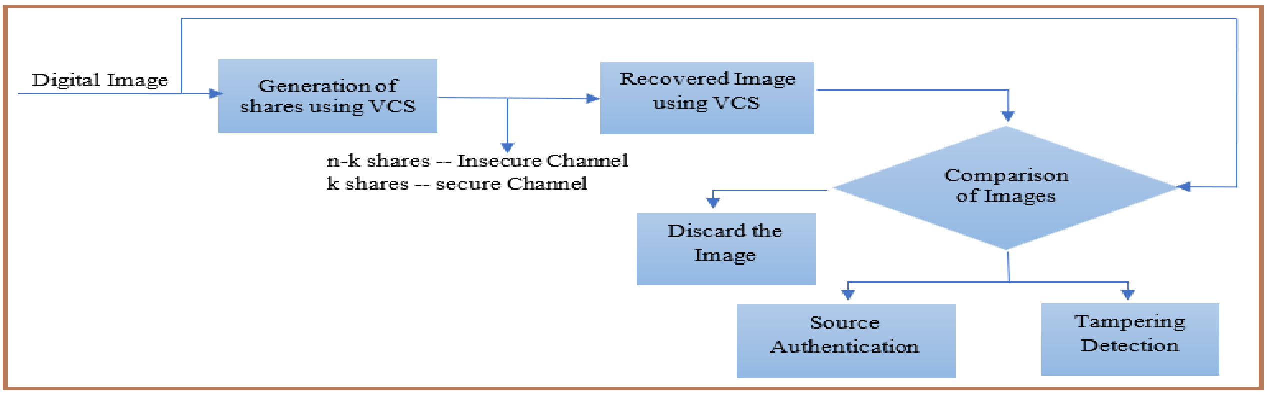
Digital Image
Generation of shares using VCS
Recovered Image using VCS
n-k shares -- Insecure Channel
k shares -- secure Channel
Comparison of Images
Discard the Image
Source Authentication
Tampering Detection

Figure 16: Proposed Active Forensic Model based on Visual Cryptography

Political dissuasions against committing to cryptographic research and practice have obscured the need for it, and it is now widely endorsed by civil libertarians, transparency activists, journalists, and computer scientists as necessary for the preservation of a liberal society in the digital age.

As a shared and distributed database for decentralised information sharing, blockchain has opened up new vistas for the use cases of distributed ledger technologies in journalism and revived hope for the industry to leverage this secure technology for the protection of intellectual property rights of legitimate writers. Calibrating the semiotics of news actors regarding one another and the semantics of covered news in the cases of Edward Snowden and WikiLeaks reveals the clarity of performances by journalists in creating their identities, particularly when the dynamics of digital news work counter the risk factor of genuine news work. Journalistic meta-discourses reveal the identities of journalists who conduct their professional news work and those who facilitate mega-leaks by merely digitally operable news content.

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

2. Scope of Information Security in Journalism

Information security in journalism anticipates numerous emerging areas of 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)* provides comprehensive coverage of contemporary information security tools, instrumentation, application, and deployment in various newsroom setups. Generally, infosec tools are evocative of surveillance activities, evasion and protection of sources on the job from private and state actors [45]. In the wake of *Journalism after Snowden,* several writers published research articles, including Carl Fridh Kleberg, who, in his reviewed article, discussed digital evasive solutions for ad hoc surveillance, source protection, safe data communication, and their storage and retrieval mechanisms, as well as 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 instils adrenaline and paranoia in journalists and their Sources, eventually hindering journalistic practices. [46]. Further Mills and Sarikakis [47] Suggests encryption Instrumentation in response to such threats. In his study, Paul Lashmar found that journalists have changed their attitudes toward source protection in the wake of the Snowden revelations and suggest the use of encryption tools; however, the efficacy of these tools has yet to be analysed. Another study of U.S. national security journalists revealed inconsistencies in their adoption of information security (infosec) tools, which further exacerbated the problem. Email encryption using PGP is used by most of them, but the whistleblowing software SecureDrop has a steep learning curve. Whistleblowing software came to the limelight after WikiLeaks' classified disclosures and several publications infatuated with the literatures about SecureDrop and GlobaLeaks. [48]. The consumer base ecosystem of information security (infosec) tools encompasses a wide range of news media organisations, from small to large, such as The Guardian and The New York Times, which are adopting 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, as well as their working with radical transparency, are 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 cyberlibertarianism and cross-border, collaborative, and secure, encrypted communication with Sources is evocative of WikiLeaks' reliance on leaked papers. [52]. State control and the territorial-technology nexus try to influence the anonymity of Sources over trans-border communication through the internet. In this perspective, also WikiLeaks seems to defend its' ground citing global communication 'freedom of the internet' beyond compromise. [53]. The use of encryption methods by 'intermediaries of change' for cross-border collaboration practices further corroborates the fact that cross-border investigations, viz. Europe's *Far Right* and *the Panama Papers leak are the result of an entente cordiale among participating nations*. Encryption requirements to evade surveillance have compelled journalists to resort to the dark web for reporting news of social significance; however, ethical considerations have raised concerns over this approach, warning that a regular presence can be fatal. African inter-continental Investigative Journalism Networks (IJN) taken as a case of country specific study for the 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 are aware of encryption strategies for 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 severe cases of corruption, are chary to leave any metadata trails behind. [56]. The amateurish adoption of infosec tools by citizen journalists for anti-surveillance activities revealed an abysmally limited understanding.

B. Individual and organizational behavior: Based on Infosec research in journalism

In this category, research is conducted that relates to individual ideas and organisational behavioural and operational needs to use infosec. Overall, the rationale and motivation for adopting information security (infosec) tools in journalism are explored under this category. In general, what journalists conjure up when listening to infosec is studied by Susan McGregor and Elizabeth Watkins [57] to develop their mental model. They concluded that 'Security by Obscurity' is the collective unconscious for almost all, so until it is entrusted and assigned to a classified job, Infosec oughtn't to be employed. However, authors later profess that such *forma mentis* is fragile and complaisant. In the US and France, infosec training and expertise rest with a 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 yielded 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 is opening new vistas for information security technocrats, focusing on strengthening the online security of existing communication tools, such as satellites, mobile phones, and other electronic devices, through routing protocols and QoS enhancements. Sharma *et al. found that there exist many inconsistencies in the Optimised Link State Routing Protocol (OLSR) used for proactive data routing in Mobile Ad Hoc Networks (MANETs*) 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 (HEVC) protocols, which facilitate lower bandwidth networks supporting smartphones and tablets, can be a new avenue of research for social science communication researchers as well. Ruan *et al. elaborated on the quality of experience (QoE) of virtual reality (VR) video streaming for* end-users. They came out with their' 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 in infallible, fortified privacy, the traditional cryptography based on DES, AES, HASH, and blockchain decentralised and distributed applications seems to succumb to the evolving research in Quantum cryptography, which uses less time for big data encryption/decryption, leveraging Quantum Key Distribution (QKD) methodology. To hedge against comprehensible digital attacks for database intrusion using quantum cryptography (QC), a post-QC approach in the form of Homomorphic Encryption (HE) is proposed for widespread use. This utilises encryption of the ciphertext and its routing over the 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. Media organisations can utilise their application for uninterruptible peer-to-peer communication, authentication, privacy, and integrity verification for other businesses, such as healthcare and private entities, who are transitioning to this evolving technology.

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

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 2017 UNESCO report recommendation for media actors and other journalism producers recommends the obligations resting on media owners to equip their investigative reporters and freelancers with sophisticated tools and training, enabling them to communicate securely with their sources on the job. A notable research area is emerging regarding the inquiry into information security 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 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 help individuals and organisations shift their behaviour to adopt InfoSec skills and attention. A notable research area emerges regarding whether individual and organisational behaviour shifts are achieved after national workshops organised for journalists’ safety, and in what frequency these workshops are organised and where. This complies with the recommendations in the UNESCO 2017 report on journalist safety.

VI. CONCLUSION

In light of the reviewed and referenced research papers accessible for information security in journalism and related fields prone to privacy and data integrity issues, it becomes apparent that as technologies become more sophisticated, new vulnerabilities emerge, highlighting their deficiencies and fallibilities. Today, as the nascent field of quantum cryptography emerges and gains prominence in the eyes of top defence governance, concerns about post-quantum cryptography are afoot, delimiting its application and raising fears about the probable abusive use of data by foreign actors to usurp government information. Homomorphic cryptography and quantum homomorphic cryptography are at the forefront, offering infallible data and information privacy and integrity. Still, the ordinary people, as well as the professionals in media and investigative journalism, need to bide their time to see the fruitful comeuppance when these technologies govern data transmission over the 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 or consent to participate, as it presents evidence that is not subject to interpretation.
Availability of Data and Material/ Data Access Statement	Not relevant.
Authors Contributions	I am 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’ sources 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.