Evolving Security Landscape of the Internet of Things: Assessing Advantages and Challenges

Syed Usman Tanveer[1], Abdul Basit Butt[2], Izhan Taha[3]
[1] University of The Punjab Lahore
[2] Tribe Consulting PVT (Ltd), Islamabad
[3] Department of Computer Science University of agricultural Toba Tek Singh Campus
Correspondence: bashibutt@hotmail.com

Citation | Tanveer S. U, Butt. A. B, Taha. I "Evolving Security Landscape of the Internet of Things: Assessing Advantages and Challenges", IJIST, Vol. 5 Issue. 4, pp 503-522, Nov 2023
Received | Aug 04, 2023**; Revised |** Oct 16, 2023**; Accepted |** Oct 24, 2023; **Published |** Nov 07, 2023.

In light of the widespread integration of the Internet of Things (IoT), it is crucial for organizations to prioritize their attention towards establishing resilient system security. The presence of any vulnerability within a system has the potential to result in system failure or a cyberattack, hence causing significant repercussions on a wide scale. This encompasses a set of measures and protocols designed to safeguard against cyber threats that especially exploit vulnerabilities in physically interconnected IoT devices. The security teams responsible for managing IoT security are currently facing a range of challenges, including but not limited to inventory management, operational complexities, variety in IoT devices, ownership concerns, increasing data volumes, and emerging threats. This review provides a critical analysis of the existing body of research pertaining to the subject of security in the context of the IoT. The focus is mostly on the present state of affairs, practical implementations, and the issues that are associated with this domain. Moreover, it delves into the prospective prospects and opportunities that are anticipated in this particular domain. Lately, there has been a noticeable surge in interest among scholars hailing from diverse academic disciplines and geographical locations, all focusing on the improvement of internet network security. The assurance of data integrity, confidentiality, authentication, and authorization is imperative in light of the substantial volume of data that traverses network devices. Nevertheless, the field of IoT security exhibits significant potential for further development. The IoT has become a popular technology paradigm that facilitates the integration of diverse objects and systems. Yet, the extensive use of the IoT has generated apprehensions regarding security, specifically pertaining to the safeguarding of data and the integrity of networks.

Abbreviations
Internet of Things (IOT)
Radio Frequency Identification (RFID)
Public Key Infrastructure (PKI)
Intrusion Detection System (IDS)
Research Queries (RQS)
Institute of Standards and Technology (NIST)
Quantum Walks (QW)
Media Access Control (MCA)
Host Identification Protocol (HIP)
Elliptic Curve Cryptography (ECC)
Authentication and Key Agreement (AKA)
Security-Enhanced Group-Based (SEGB)
Vehicle-to-Grid (V2G)
Software-Defined Networking (SDN)
Peer-to-Peer (P2P)
Wireless Sensor Network (WSN)
Enhanced Security Wormhole Intrusion (ESWI)
Wireless Sensor Network (WSN)
Internet Protocol Security (IPSEC)
Data Authentication and En-Route Filtering (DAERF)
Distributed Anonymous Entity Framework (DAEF)
Data Centre (DC)
Information Security Management (ISM)
Low-Energy Adaptive Clustering Hierarchy (LEACH)
Cognitive Radio (CR)
Simultaneous Wireless Data and Power Transfer (SWDPT)
Primary Users (PUS)
Secrecy Sum Rate (SSR)
Squared Residuals (SR)
Industrial Internet of Things (IIOT)
Home Area Network (HAN)

Keywords: Internet of Things, Network Security, Confidentiality, Authentication

Introduction:

The advent of the twenty-first century has been accompanied by significant advancements in computer networking, representing a period defined by the proliferation of wireless communication and interconnection. The phrase "Internet of Things (IoT)" is a modern technological innovation that enables the creation of networks that connect many entities, including both physical and virtual domains [1]. The IoT encompasses a wide range of devices, spanning from compact wearables to expansive machinery. These devices are connected with actuators and sensors, which empower them to intelligently perceive their environment and react independently. The growing utilization of IoT applications and devices is expected to rise due to their expanding adoption across various sectors. The commercial operation under consideration is to the supply of wearable technology, specifically devices designed to monitor and transmit an individual's behavioral and health data [2]. In the healthcare sector, patients are being furnished with applications and gadgets based on the IoT. The current assortment of IoT products designed for smart homes includes a diverse array of devices, such as intelligent refrigerators, automated heating systems, advanced gardening solutions, video doorbells, lighting control personal assistants, automated coffee makers, and sophisticated door locking mechanisms [3].

The subject of security has garnered considerable interest within the academic sphere. The current topic of study has received considerable interest in academic circles, IoT comprises a multitude of advantages, yet it is not devoid of substantial obstacles, specifically pertaining to data transfer, data harvesting, and data security. These devices have the potential to establish connections with pre-existing networks and ease the interchange of data. The achievement of this outcome is facilitated by the implementation of numerous protocols that have undergone iterative development and refinement to efficiently transmit the gathered data [4]. However, these protocols do not receive the requisite level of attention they merit. Login issues can lead to various security breaches, including denial of service attacks, replay attacks, Denning-Sacco attacks, password guessing attacks, and other similar incidents. On the other hand, the process of verifying the authenticity of IoT devices across networks that are varied and interconnected presents considerable difficulties. The protocols should also include the issues associated with the limitations of IoT applications, including energy consumption, constrained memory space, and limited processing capacity [5].

The present scholarly work offers a thorough analysis of the progression, utilization, and obstacles pertaining to the IoT. The implementation of a layered approach has attracted attention to the security risks associated with the IoT. A comparative investigation was undertaken to improve the security of the IoT by evaluating anomalous detection approaches against the most recent version of the Intrusion Detection System (IDS). IoT encompasses many types of assaults that can be mitigated by the utilization of authentication techniques and lightweight encryption algorithms. The authors posit that additional inquiry is imperative to augment the security of IoT widgets. The current study, put forth a design framework that prioritizes cybersecurity measures across four distinct layers [6]. This framework aims to effectively address security concerns inside the realm of the IoT. The objective of their research was to investigate and categorize different forms of cybersecurity assaults that specifically target IoT platforms. The discourse centered on the utilization of the previously stated entity across various industries and the deployment of defensive strategies against attacks. This study, included device security, transmission security, and data security as components under their taxonomy of security criteria for evaluating the security of IoT systems. The study examined the difficulties faced in different implementations of the IoT and put forth feasible security methods to address these concerns [7].

The study presented a thorough and practical set of suggestions for enhancing the

infrastructure of the IoT with the aim of enabling secure interactions and conducted a thorough analysis of the security problems and potential vulnerabilities that are inherent in IoT applications. The attainment of this objective is accomplished by prioritizing vulnerabilities that have the potential to result in a security breach [8]. This includes the recognition of overarching threats and attack vectors that specifically target IoT devices. The primary security benefits associated with each of these systems are their inherent flexibility and scalability. The inquiry also examined the security requirements and issues linked to various IoT applications. The existing security alternatives can be classified into two primary categories: traditional procedures and innovative ways [9].

Paradigm Behind this Study:

Prior research in the domain of literature has primarily concentrated on examining the security dimensions of the IoT. The primary objective of this study is to evaluate the existing research on security and the IoT, specifically highlighting the utilization and challenges associated with data security within the domain of network security [10] [11]. One of the foremost obstacles in guaranteeing the security of the IoT is to the authentication and authorization of devices in order to obtain network and data access [12]. The paramount significance lies in safeguarding these devices against physical assaults, a goal that can be accomplished by the utilization of tamper-resistant hardware and the execution of secure installation processes [13].[14]

The debut of a remotely controllable toaster in 1990 served as the inaugural milestone in the development of the essential devices under the classification of the IoT. The emergence of a system that utilizes Radio Frequency Identification (RFID) technology for the purpose of item identification is well-documented in the literature. This smart device application gained prominence approximately ten years after its initial development. The rapid expansion of IoT intelligent applications have greatly transformed the domain of network technology. The applications of intelligent banking, intelligent grids, intelligent health care, and other intelligent services serve as prime examples of their utilization. The introduction of several applications of the IoT has led to substantial transformation in the sector [15]. The integration of the IoT in the industrial sector spans diverse domains, among which predictive maintenance holds notable importance. Within this particular context, the utilization of IoT sensors assume a pivotal function as they engage in the ongoing surveillance of various equipment and machinery. This constant monitoring facilitates the identification and subsequent detection of maintenance requirements. In a consequence, this methodology reduces the amount of time that systems are not functioning and improves the overall effectiveness of operations. The IoT sensors possess the capacity to actively monitor and track various assets, such as items, containers, and cars, in a live and continuous manner. This feature boosts the visibility of the supply chain and provides enhanced control over the movement and management of these assets [16] [17].

The industrial sector derives advantages from a diverse array of IoT applications, which play a role in diminishing costs, enhancing productivity, and optimizing efficiency. The continuous progression of technology suggests that the industry is likely to experience additional improvements in IoT applications, characterized by heightened levels of innovation. It is imperative to acknowledge, though, that the incorporation of the IoT inside the industrial domain poses a range of obstacles. These challenges encompass significant costs associated with establishing IoT infrastructure, concerns regarding data security and privacy, and the need for specialized expertise and skills in the construction and maintenance of IoT systems [18]. It is imperative for industries to conduct a comprehensive assessment of the advantages and constraints linked to the adoption of IoT. The extant corpus of scholarly literature has witnessed numerous scholarly contributions; nonetheless, the limited quantity of available

research hinders the attainment of a thorough and multifaceted comprehension of security analysis. It is imperative to conduct a thorough examination and evaluation to rectify this discrepancy. The comprehensive analysis should not exclusively concentrate on issue identification, but should also incorporate an exploration of potential solutions within a broader conceptual framework [19].

Network Security:

The subject under consideration concerns the security prerequisites within the domain of the IoT [20]. The notion of information assurance is the deployment of strategies aimed at guaranteeing the dependable and secure operation of information systems, while concurrently preserving and defending the information stored inside them. According to the National Institute of Standards and Technology (NIST), information assurance encompasses a collection of methodologies aimed at ensuring the confidentiality, authenticity, integrity, availability, and non-repudiation of both data and information systems [21]. The processes stated above involve the incorporation of security, detection, and reaction capabilities in order to facilitate the restoration of information networks [22].

The use of strong authentication and access control methods is crucial for safeguarding the security of the IoT ecosystem. These steps are of utmost importance in preventing unauthorized access and protecting against potential cyber dangers [23]. In addition, it is crucial to utilize encryption and strong security protocols in order to protect the data generated by IoT devices, thereby ensuring the maintenance of privacy and confidentiality. Moreover, it is crucial to ensure the protection of data from unauthorized alterations to maintain its integrity and authenticity. The safeguarding of networks and devices is an essential element within the realm of IoT security. Ensuring the security of systems within IoT against network-based assaults is of utmost importance [24]. The mitigation of physical attacks, which includes acts of vandalism, theft, and tampering, can be efficiently tackled by implementing security mechanisms that are incorporated inside IoT devices. The given text does not include enough information to be rewritten in an academic manner. Kindly furnish a more comprehensive discourse on the subject matter, which pertains to network security [25].

Internet of Things:

The IoT is a technological framework that enables the integration of physical objects with internet access, hence enabling intelligent collaboration between these objects and their surrounding environments. Thus, these applications are frequently utilized across various environments in order to accomplish a diverse array of goals [26]. The complex character of IoT ecosystems is attributed to the incorporation of transdisciplinary elements, networks, computational processes, and other associated aspects. To meet the projected security requirements of the IoT, it is crucial to establish a holistic solution that incorporates all pertinent factors and maintain compliance with security prerequisites. However, IoT devices are frequently employed in highly populated and unregulated settings, enabling individuals with malicious intent to gain unrestricted access to these devices [27]. The interconnection of these devices through wireless communication networks exposes a notable vulnerability that can be exploited by malicious individuals. These malicious entities possess the capability to assume the identities of eavesdroppers, so acquiring unauthorized entry to confidential data transferred across communication networks. The limited resources of IoT devices are considered as the primary reason for their inability to support complex security measures [28]. However, this convenience also increases the vulnerability of internet systems to numerous forms of attacks [29].

The widespread use of IoT devices has led to the generation of substantial amounts of data. This data is subsequently transmitted across networks, making it susceptible to potential cybersecurity threats [30]. The safeguarding and preservation of data's security and

authenticity. Information assurance refers to a detailed categorization of security criteria or objectives that are specifically applicable to particular digital information systems. Consequently, this specific section offers a comprehensive examination of the goals and/or requirements related to the security of IoT systems. This paper additionally presents an examination of the issues encountered in satisfying the standards for industry 4.0 applications. It elucidates the underlying reasons for the difficulties faced in meeting the security requirements through conventional approaches [31]. The security needs can be succinctly summarized as follows: Within the digital domain, the significance of data security is now widely acknowledged as an essential component of comprehensive security measures. The emergence of the IoT necessitates the incorporation of robust data security measures as a fundamental aspect of constructing secure internet networking systems. Several researches have indicated that ensuring data confidentiality is a crucial security need for IoT data. Nevertheless, within industrial environments, the need of maintaining data integrity and ensuring data availability surpasses the importance placed on maintaining secret [32]. The primary factor contributing to this phenomenon is the palpable impact exerted by these entities on the functioning of corporations. The viewpoint expressed is considered unsuitable in the context of a culture that heavily relies on networked devices, since businesses are swiftly converting their conventional offline systems into internet-based frameworks. According to surveys done within enterprises, it has been empirically demonstrated that the protection of data serves as a prominent motivator for firms to adopt Industry 4.0 [33]. In the early phases, it is widely recognized that organizations hesitate in using cloud servers as a method for storing and exchanging data over internet networking sites [34]. Nevertheless, it is crucial to acknowledge that the majority of occurrences of IoT data breaches predominantly occur within commercial entities rather than at cloud service providers. Following this, the advent of cloud-based storage evolved as a strategy to address the susceptibility to security breaches in both corporate and cloud environments. However, the urge to mitigate data loss has become increasingly important, requiring the identification of four crucial steps necessary for the development of a successful solution. These elements involve the processes of identification, prevention, recording, and notification [35].

The issues within this particular domain are intricately linked to the convergence of three variables. In light of the limited resources and mobile nature of IoT systems, it is imperative for data security approaches to operate in a manner that optimizes resource utilization. In addition, numerous infrastructures within the IoT system are dependent on the interchange of data. However, in contexts where the protection of data sensitivity is of utmost importance, ensuring secrecy becomes a primary concern, often giving rise to a variety of obstacles [36]. Moreover, there exists a notable increase in the need for safeguarding data integrity, particularly in relation to essential IoT services or applications. IoT security pertains to a defensive approach that aims to protect physically interconnected IoT devices from deliberate and focused attacks. The protection of network infrastructure and sensitive data against unauthorized access, hostile assaults, and potential harm is of utmost importance, making network security an essential component [37]. Encryption methods are a specific aspect encompassed by the wider domain of data protection. The convergence of the IoT and the Industry 4.0 framework offers numerous benefits, including the improved utilization of data generated by IoT devices. This includes the transmission of information and other procedures that depend on data, which may take place either within or outside the confines of the organization. The following section of this paper illustrates additional information concerning different methodologies for guaranteeing the confidentiality of IoT data, in conjunction with encryption methods [38]. The mitigation of cyberattacks is a critical concern in safeguarding the security of internet devices and networks. The responsibility of network

security lies in the protection of interconnected networks that enable communication among internet applications. Ensuring the security of the complete IoT ecosystem encompasses the protection of devices, networks, and applications against potential cyber threats [39].

Data Security:

Data security is a set of precautionary measures that are put in place to safeguard the confidentiality, integrity, and accessibility of data that is gathered and transferred by IoT devices. This procedure involves the encryption of data while it is being transmitted and the subsequent secure storage of the encrypted data. In addition, the incorporation of access restrictions and authentication mechanisms plays a crucial role in reducing the potential for unauthorized entry to sensitive data [40]. The implementation of data security protocols is of utmost importance in ensuring the protection of data obtained and transmitted by internet networks [41]. The susceptibility of IoT devices to cyber assaults underscores the need for the adoption of various safeguards, including network security, cybersecurity, and data protection measures, to effectively safeguard these devices. The research methodology encompasses the systematic strategy utilized by scholars to explore and collect data in order to address research inquiries or examine hypotheses.

Research Methodology:

This review study follows established standards and methodologies for conducting systematic reviews, as indicated in previous systematic review studies [42]. The following subsections provide a succinct overview of each phase. The primary aim of establishing these criteria is to ensure the selection of studies aligned with the research scope for subsequent analysis. The selection of specific research articles for investigation adhered to the inclusion-exclusion criteria specified [43].

Table 1: Inclusion and exclusion criteria formulated for execution of this review

Inclusion Criteria	Exclusion Criteria
Should include terms related to data privacy, communication systems, data transfer, acquisition, sharing, and confidentiality	Articles in press and not written in English
Document should be an article and its source should be a journal	Duplicates

Data Collection and Search Strategy:

A comprehensive investigation was conducted using the Scopus and Google Scholar databases. The initial step in the search strategy involved identifying key search terms that served as the foundation of this inquiry. The search query comprised diverse combinations of keywords, including "Internet of Things" and "Network Security," as well as alternative terms such as "IoT" and "Network." The careful selection of appropriate terminology at this stage of the systematic review significantly influences the papers considered for analysis. The terms mentioned above resulted in a total of 510 retrieved documents. The presence of duplicate entries necessitated the removal of 40 records, leading to a total of 450 articles for evaluation. Subsequently, the data segments were examined and filtered in accordance with the predefined inclusion and exclusion criteria [44]. As a result, a thorough analysis was conducted on a total of 20 papers that met the specified criteria.

Results:

IoT software platforms can be defined as software components that enable the seamless exchange of data and services among interconnected IoT devices within a network. These platforms encompass various aspects, including data acquisition, integration, storage, monitoring, security, event handling, application support, data analysis and visualization, device management, as well as connectivity and network administration. The security solutions

for networked IoT systems can be categorized into four distinct areas [45], which involve ensuring data integrity during transmission, securing data storage, verifying and authorizing devices attempting to connect and transmit data, and validating the identities of individuals or organizations. (IoT) software platforms can be broadly classified into two categories: cloud-based platforms and open-source platforms. Over time, the IoT industry has proactively addressed potential risks and vulnerabilities by developing security solutions tailored to safeguard IoT systems and devices. In recent years, regulatory bodies and manufacturers have increasingly emphasized the importance of securing IoT devices. This is evident in the gradual growth in the number of academic articles published over the past decade [46].

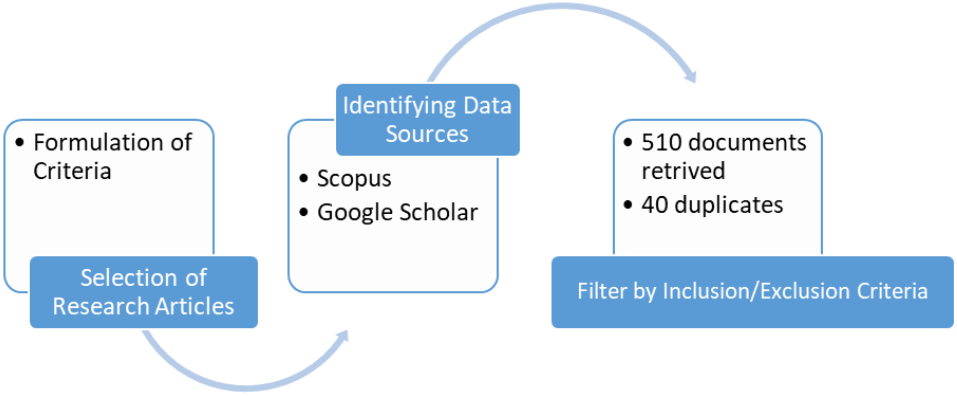

Figure 1. Research methodology employed.

Result and Discussion:

A network is formed by connecting devices together in order to carry out designated functions. Both traditional and cellular networks are considered to be feasible alternatives. The acquisition and transmission of valuable knowledge aided by network connectivity might provide individuals with potential advantages. The utilization of network infrastructure is crucial for facilitating the efficient transfer of data. The notion of information security applies to an organization's goal of protecting data while it is being transmitted across a network. According to prior research the three primary goals of information security encompass the preservation of data confidentiality, the assurance of data integrity, and the regulation of data access exclusively to authorized personnel. The examination of data security in the realm of the IoT and cloud computing is a nascent field within the broader discipline of computer security. The present topic has the potential to leverage the current knowledge and insights derived from the established domain of data flow management for security [45]. In the realm of data security, the inherent partial orders have performed a pivotal and satisfactory function. Within a given network, entities exhibit varying levels of secrecy or integrity, which are dependent on their place within the partial order. The research presented in this paper focuses on the development of labeling systems that efficiently assign security criteria to precisely locate elements within network partial orders. The incorporation of illustrative instances effectively demonstrated well-established concepts in the domain of data security, encompassing disputes, aggregation, and consolidation. The demonstration involves illustrating how entities in incomplete orders can be updated through actions done by users or managers, including addition, deletion, or relocation.

To establish a robust and protected end-to-end connection across various services, it is crucial to effectively tackle the multitude of security concerns linked to current communication technology. Furthermore, the current security mechanisms that are often perceived as reliable may be susceptible to possible vulnerabilities given the recent and rapid progress in quantum technologies. Therefore, in order to adequately mitigate prospective quantum computer attacks, contemporary security systems must feature resilient quantum

technology. The study conducted introduces a new and efficient approach for encrypting images, utilizing the concept of QW. The purpose of this approach is to augment the level of security in the transmission of data within IoT systems and wireless networks that use edge computing. The methodology under consideration involves the construction of permutation boxes by using the non-linear dynamic characteristics of QW. The analysis of inter-pixel correlations is unachievable in determining the content of encrypted images, mostly due to their intrinsic random nature. In addition, the entropy value is estimated to be 8, suggesting a greater proportion of pixels experiencing alterations.

The major parameters demonstrate a notable degree of sensitivity, featuring a substantial critical region that can survive diverse types of attacks, reaching a level of 99.61 %. Li et al. presented a data security monitoring system that employs narrow-band IoT technology. The objective of their study was to address the difficulties related to the erroneous classification of data and the constrained efficacy of conventional data monitoring methodologies. The first stage in the data collecting process for the intranet was the creation of a model for network data collection and the determination of the most effective configuration for a sensor node. The development of dynamic intranet data analysis indexes was conducted based on three separate perspectives, which were developed through an examination of the data's characteristics. The findings from the conducted tests demonstrate that the suggested methodology continuously attains its desired objectives in relation to accuracy rate, with a performance surpassing 90%. Additionally, the classification time remains below 4 seconds, and the energy consumption remains below 150 Joules. These outcomes remain consistent regardless of the occurrence or absence of a network attack.

The IoT frequently offers crucial services for the creation of applications, encompassing data collection, management, as well as device and data security. This encompasses a range of devices or gadgets that actively engage in interactions and computations, with the primary objective of augmenting the convenience and security aspects of our everyday existence. The IoT possesses the capacity to facilitate the automation of inventories, allowing for real-time monitoring of things, and aiding in the administration of information and state relevant to diverse objects. In order to facilitate the transfer of a substantial amount of data between network devices, it is imperative to develop a robust security architecture that guarantees the maintenance of data integrity, confidentiality, authentication, and authorization. The matter of security in the IoT is progressively presenting a substantial obstacle for security experts as they endeavor to reduce susceptibility to malicious attacks. The presence of numerous security vulnerabilities in Mobile devices requires the construction of a data routing system to enable the transmission of collected data. The proliferation of IoT technology has resulted in substantial alterations to the daily routines of citizens in various countries, hence generating a profound worldwide influence. The protection of IoT networks requires security procedures similar to those employed for other software programs, as the data they produce frequently includes sensitive information. The current security mechanisms implemented in these networks are insufficient in effectively addressing all security objectives. The prompt emphasizes the necessity of promptly implementing protective measures to safeguard data against many forms of attacks upon its identification within the domain of the IoT. In addition, it is crucial to ascertain the attainability of data integrity, access control, confidentiality, and authentication for all pertinent entities.

The internet systems possess several significant attributes that warrant attention in the realm of security-conscious routing. These attributes encompass a multi-hop autonomous architecture, dynamic topology alterations resulting from mobile IoT devices, limited connection duration, delays in media access, and susceptibilities to security breaches across multiple layers. Consequently, these characteristics engender ongoing discussions regarding

the need for security-conscious routing in the IoT domain. The utilization of cross-layer routing becomes essential in order to optimize network efficiency by picking the most efficient routing choice. The incorporation of dependency factors as routing parameters across different protocol levels has been seen established a secure cross-layer protocol design that employs routing parameters obtained from data exchanged at the Media Access Control (MCA) layer. The SI-SLnO technique takes into account many restrictions, such as distance, energy consumption, and risk factors associated with a given route, in order to make well-informed decisions regarding routing. The risk component was calculated for each ideal path. The assessment of data privacy requirements was conducted by adopting threshold-based risk factor utilization, utilizing Elliptic Curve Cryptography (ECC) and the Elgamal cryptosystem. Various measurements were utilized to validate the superiority of the proposed secure cross-layer protocol. The constrained access to energy and computational resources in IoT devices is a substantial obstacle for doing research on communication security and hacking within these networks. The urgency to reduce energy waste arises from the significant power consumption associated with effective security systems. The utilization of optimized application-specific security protocols is a common strategy to improve the efficiency of data transport while simultaneously maintaining a strong level of security. It is imperative that the optimization process does not have any negative impact on the functionality of the security measures that are in place, such as confidentiality, integrity, and authenticity. The Host Identification Protocol (HIP) is a security method that was being optimized for use in the host identification protocol by Kanuch and Macko. Numerous opportunities for enhancement have been found, and a subset of these have been integrated into the proposed E-HIP optimized method, subsequent to a comprehensive review of pertinent literature. The Open HIP module, which is an open-source software component, has been customized and deployed to facilitate the establishment of a link between physical hardware devices. This adaptation has been made specifically for the purpose of conducting testing. The process of encrypting the transmission was successfully conducted. The experimental evaluation has revealed that the proposed optimization technique yields a notable enhancement in energy efficiency, with an estimated rise of 20%have put forth a range of group-based Authentication and Key Agreement (AKA) strategies in the extant literature, with the aim of attaining authentication. These techniques effectively meet all established security standards, but not limited to privacy protection, reciprocal authentication, integrity, and secrecy. However, none of them possess the necessary qualifications required to effectively handle the principal difficulty encountered by the information network. Moreover, these methods are vulnerable to widely recognized attacks and demonstrate insufficient effectiveness in preserving the unlinkability of the group key. The implementation of certain protocols requires the individual identification of each communication device belonging to a particular machine type in order to enable simultaneous access to the communication network. This process, however, leads to an additional burden on the network in the form of increased congestion. The SEGB-AKA protocol successfully accomplishes the objectives of ensuring both forward and backward confidentiality of keys, while also mitigating the drawback associated with the dependence on a solitary key throughout the authentication procedure. The research findings demonstrate that the protocol demonstrates enhanced performance in relation to network overhead and effectively fulfills the predetermined requirements.

This response will delineate the various variables that are crucial for guaranteeing security in machine-to-machine communication.The first determination of the optimal quantity of authorized access requests was conducted in a dynamic way for each Vehicle-to-Grid (V2G) network domain. The objective of this endeavor was to effectively establish a system for access admittance control that takes into account capacity-related considerations,

including the potential for overload, limitations in system capacity, and the mobility of electric vehicles. To ensure the implementation of robust access authentication measures and to ensure that sessions are only conducted by authorized individuals, a comprehensive authentication model incorporating specific authentication protocols was adopted. The primary objective of this activity was to facilitate reciprocal authentication and ensure the preservation of data confidentiality inside defined sessions. The accomplishment was attained through the process of confirming the presence of preexisting data concerning the reliable linkage between the relevant V2G network domains. The discourse also addressed the subjects of effective session termination with forward security and session recovery without the necessity of an additional verification delay. The presentation of the analytical and assessment outcomes was conducted with the purpose of showcasing the effectiveness of Access Auth. The methodology can be utilized to construct a comprehensive database, enabling anyone to examine, organize, and efficiently utilize the data. It is anticipated that the use of this methodology will improve the reliability and availability of the data, hence leading to improved service delivery for consumers. The primary aim of the study done was to design and construct a data exchange protocol that is both unique and dependable, with the ultimate goal of ensuring the security of data transfer. The main area of research pertains to the examination of dependability and the validation of trade process behavior. The anti-interference and security authentication method is evaluated through a simulation experiment, which is conducted after analyzing abnormal phenomena in IoT traffic, understanding the principles of network traffic, constructing an anti-interference model for multi-terminal power communication networks, and establishing a noninterference model. The findings of the research demonstrate that augmenting the quantity of antennas resulted in a reduction in the likelihood of erroneous detection, decreasing it from 10−1 to 10−4. The enhanced precision leads to improved efficiency in the identification of active users. HTTP Plus SSL has become the prevailing protocol for data verification and security authentication in network environments. The sector pertaining to anti-interference technology has undergone significant growth. The global market has witnessed a substantial rise in its annual growth rate, nearly reaching twice its prior worth. Furthermore, there has been a significant expansion in the size of the market, with an annual growth rate of roughly 50%.

The IoT plays a substantial role in the practical domain by offering autonomous support for operational and communication functionalities. This allows for the facilitation and maintenance of sophisticated services that are commonly utilized in daily activities. To effectively address the diverse range of threats targeting IoT networks, it is imperative to conduct a thorough analysis of security protocols in forthcoming iterations of IoT and devise sophisticated strategies to uphold confidentiality. The blockchain technology has emerged as a viable alternative for providing notable attributes such as enduring confidentiality, authentication, and resilience. introduced a distributed security architecture in their research, which integrates Software-Defined Networking (SDN) and edge cloud technologies, while also incorporating blockchain functionality. The mitigation of security attacks targeting the edge layer of the IoT network is facilitated by the deployment of security attack monitoring mechanisms at the cloud layer. The utilization of SDN has allowed for the facilitation of network traffic flow management in a dynamic fashion through the implementation of a gateway. The aforementioned capacity demonstrated its advantageous nature in the process of identifying security assaults through the detection of network traffic flows that exhibited suspicious characteristics. Moreover, it successfully reduced security attacks by hindering the advancement of these questionable streams. The findings suggest that the security architecture described in this study successfully addresses the issues pertaining to data confidentiality that arise from the convergence of the SDN paradigm, edge cloud, and blockchain technology.

One aspect of concern within IoT sector relates to meeting the urgent requirements of modern consumers for dependable transmission services, given the swift proliferation of IoT technologies inside the information society. The issue of ensuring the security of data exchange and transmission over internet networks has continually presented difficulties introduced an innovative security authentication methodology for the IoT in their scholarly article. This approach combines a dynamic Bayesian network with a robust protocol, effectively tackling the existing research gap in authentication for IoT security. The network has successfully incorporated a robust measurement and integrated security verification system based on public key cryptography to aid users of the IoT in choosing a data transmission route that ensures both a high level of security and reliability. Consequently, there was an enhancement in the dissemination of security information and the determination of routing alternatives, as it incorporated the assessment of node credibility and path dependability. The evaluation findings suggest that the method employed in real-time applications demonstrates greater performance in terms of overhead and computational complexity when compared to other algorithms. The application shown a high level of adaptability and effectively responded to a denial-of-service assault, thereby reducing the risk presented by abnormal Internet of Things entities. The incorporation of blockchain technology into Peer-to-Peer (P2P) networks has presented a viable structure for the advancement of IoT and Beyond 5G applications. The incorporation of a distributed architecture and security services within the network enabled an enhanced range of financial activities, hence offering a significant benefit. One of the primary observations in IoT-based networks is the existence of a diverse array of IoT devices, accompanied with notable security concerns and obstacles related to energy consumption. The adoption of several blockchain technologies, specifically public blockchain for P2P communication and private blockchain for SDN, is regarded as a feasible strategy. The system has been enhanced with the integration of an extra component. This component enables the sender to digitally sign the specific action during the data transfer process between two users. The primary objective of this integration is to bolster confidentiality and mitigate the risk of repudiation. Public-key value-based signatures are produced by employing the private key of the transaction and afterwards revealed in conjunction with it. The confirmation of the action was achieved by the nodes utilizing a signature that is based on the value of the public key that was generated. The utilization of hashing in encryption provides an increased level of immutability. When compared to the approaches now in use, the findings of this study demonstrated a higher level of performance in terms of speed and reaction time. Additionally, there was a notable decrease in both end-to-end latency and overhead. Additionally, the research findings demonstrated the implementation of heightened security protocols during the process of data transfer. The project employed the Pyethereum testing utility, a constituent of the Ethereum platform. In their publication, introduced an innovative security methodology designed specifically for dispersed IoT systems. ChaCha20 is widely acknowledged as the dominant lightweight encryption method in modern cryptographic frameworks. To augment security and increase the degree of unpredictability, the generation of random numbers is implemented by utilizing ideas derived from cellular automata. The posting and saving operations were enhanced with the implementation of many layers of data protection, achieved by utilizing double encryption. Moreover, it serves to uphold the authenticity of communications, accelerate the process of execution, authenticate users, and enable the secure exchange of data among various communication entities. The successful completion of the registration process is of utmost importance for the IoT device that is connected to the gateway server.

The efficacy of the proposed concept was demonstrated. Wireless networks encompass communication technologies that facilitate the transmission of data and

information without necessitating physical connections or wires. Wireless sensing networks are of paramount importance in the context of the IoT and have been widely employed in several fields of human activity. The process of verifying identity in wireless sensor networks is an essential mechanism that ensures users can securely access real-time data generated by sensor nodes. This method plays a significant role in limiting potential dangers. In the context of an IoT enabled Wireless Sensor Network (WSN), a multitude of small-scale sensors are utilized to gather data and afterwards transmit it to centralized repositories. The sensors, which rely on battery power and possess finite resources, direct a substantial proportion of their energy towards the functions of detecting, gathering, and transmitting data. The matter of security poses a substantial apprehension within these networks during the transmission of data, owing to their vulnerability to a range of attacks, with the wormhole attack being the most severe. The commencement of these attacks takes place without the acquisition of crucial network information, so presenting substantial dangers to the effectiveness, security, and communication of the network. T The ESWI (Enhanced Security Wormhole Intrusion) methodology was devised with the aim of enhancing both efficacy and security in the identification of wormhole attacks. The intentional simplification and reduction of complexity in the design of this method aim to minimize operational overhead and energy consumption. The simulated outcomes of their approach demonstrated comparable levels of detection rates and packet transit ratios. Moreover, it resulted in a significant decline in energy usage, a drop in the duration of end-to-end communication, and an improvement in overall performance. Wireless sensor networks, which are a crucial element of the IoT, have a wide range of applications in several fields of human life. The process of identity identification is crucial in enabling users to safely retrieve real-time data from sensor nodes within wireless sensor networks. A Wireless Sensor Network (WSN) based on the IoT is utilized to collect data and send it to a centralized storage system. The central emphasis of energy utilization in these devices, which rely on battery power and possess restricted resources, is oriented towards the activities of data detection, collecting, and transmission. The security aspect holds significant importance in relation to the exchange of data within these networks, as they are susceptible to many dangers, with tunnel assaults being the most severe.

To guarantee the preservation of data confidentiality, integrity, and availability, it is crucial for IoT devices equipped with IPv6 to possess interoperability with the Internet Protocol Security (IPSec) protocol. The principal aim of doing a port check is to augment the security of Internet of Things (IoT) devices. However, it is crucial to acknowledge that this procedure might potentially detrimentally affect the performance of IPSec services, particularly in relation to network speed. IDPS is employed to enhance the security of internet devices over the IEEE 802.11ah WLAN. proposed unique mathematical models for the assessment of security in the IoT.

The models in question have determined an optimal scanning rate for security administrators by taking into account the usage of IPsec services and the performance of port-scanning networks. Furthermore, it is important to acknowledge that the existing solutions lack the inclusion of built-in verification as a distinctive attribute. Therefore, the study conducted introduced a robust and effective framework for the IoT by leveraging WSN technology. The COOJA simulator was utilized to conduct a comparative analysis between the suggested security strategy and the currently implemented security systems, specifically SPECK and SIMON. The proposed methodology demonstrated superior performance in comparison to alternative approaches. It achieved a reduction of 2% in CPU cycles, a decrease of 10% in execution time, a 4% decrease in memory needs, and a minimum improvement of 10% in security efficacy.

The two-factor authentication method described employs an elliptic curve cryptosystem and its security is validated through the utilization of the formal proof tool ProVerif. The proposed methodology demonstrated superior security compared to analogous strategies, while concurrently upholding acceptable levels of computational cost effectiveness. Dong Chen et. Al, proposed a novel verification methodology that was specifically tailored for Wireless Sensor Networks (WSNs). The proposed methodology successfully tackled common obstacles and showcased its compliance with IoT security properties, specifically when compared to some contemporary schemes concerning WSN security characteristics. The technique known as Data Authentication and En-Route Filtering (DAERF) for WSNs within the framework of the IoT was proposed. According to their security analysis, it was concluded that the DAEF shown proficient capabilities in mitigating node compromise and denial of service attacks. These assaults primarily aimed at disrupting reports and selectively sending data were effectively countered by DAEF. Furthermore, a comprehensive analysis of energy use was carried out alongside the assessment of the benefits of DAEF in relation to similar schemes. The devices within the WSN situated at the Data Centre (DC) in the Energy Internet of Things (EIoT) demonstrated vulnerability to attacks and were susceptible to encountering difficulties associated with Information Security Management (ISM), such as suboptimal real-time performance and considerable complexity. presented a comprehensive elucidation of the structural arrangement of a DC WSN designed specifically for the EIoT. Simulations were performed on a WSN utilizing the Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol. These simulations were used to make predictions regarding various forms of attacks. The aforementioned data was employed in the creation of a dynamic and real-time strategy for the WSN in the context of ISM. The present study focused on enhancing the framework and methods of LEACH, a widely recognised protocol in the field of wireless sensor networks. Furthermore, the utilization of information fusion techniques was implemented in order to mitigate the magnitude of data transfer. The efficacy of the proposed approach in ensuring communication between nearby nodes and between higher and lower levels was proved through the findings of a simulated exercise. Furthermore, it enhanced the robustness of network security by including timely key updates, and promoted streamlined data transmission through the mechanism of information fusion.

Investigated many facets of key management in the context of mobile IoT by employing a widely recognized identity cryptosystem. The initial allotment of storage is established as 32 bytes and later increases to 84 bytes during the first stage of registration, 82 bytes during the second stage of registration, and 356 bytes during the third stage of authentication. This expansion is a result of an augmentation in the number of bytes required for login authentication. This approach has demonstrated several advantages in terms of enhancing safety performance. The researchers conducted an analysis in their work on secure beamforming for a two-way Cognitive Radio (CR). conducted a study to examine the benefits of Simultaneous Wireless Data and Power Transfer (SWDPT) in the context of an internet network. The IoT manager, located centrally within the secondary network, utilizes the primary spectrum to facilitate the transmission of data and provision power to the remaining IoT devices. Furthermore, it offered relay support and implemented joint physical layer protection mechanisms to mitigate the risk of eavesdropping for two Primary Users (PUs). The objective of the study was to improve the level of information security by optimizing the Secrecy Sum Rate (SSR) for PUs using a collaborative approach involving the design of the beamforming matrix and vectors at the central controller. The initial concept entailed employing a branch-reduce-and-bound-based technique to effectively tackle the nonconvex problem. The process involved in this study consisted of determining an upper limit for the sum of Squared Residuals (SR) and presenting a practical solution through Gaussian

randomization. Nevertheless, the complexity of the procedure was increased by the necessity of incorporating two layers of repetition. The authors presented the simulation results to showcase the relative efficacy of their proposed optimization tactics compared to established methodologies.

In the domain of network engineering, there has been notable progress in the Industrial Internet of Things (IIoT), leading to a rise in the occurrence of data leakage problems within networks on a yearly basis. A revolutionary anti-intrusion monitoring device has been developed to boost the security defense of IIoT systems while adhering to privacy regulations. The implementation of the IoT requires strict adherence to stringent standards in its structural system. Additionally, it necessitates the implementation of robust security performance criteria in an environment that is distinguished by potential network threats. The network system should adopt a methodology that is characterized by a limited occurrence of data loss and a high level of stability developed an early deep-learning network technology by a thorough assessment of various network topologies. The utilization of Convolutional Neural Network technology was employed to improve and refine the LeNet-5 network, leading to the creation of a fresh LeNet-7 model. The development of a comprehensive system for monitoring and preventing intrusions in the IIoT was achieved through the integration of three independent network technologies. The effectiveness of the system was evaluated and confirmed. The algorithm demonstrated a high degree of accuracy in detecting the desired outcomes, with a low incidence of false-positive results, and revealed a noteworthy level of precision in data handling. In order to improve performance, the study assessed the model's ability to handle high-performance data and contrasted it with privacy-aware task offloading schemes. Therefore, the implementation of this technology has the capacity to ensure the safeguarding of data confidentiality within the framework of IIoT in compliance with pertinent legal regulations.

The delivery method within the hospital information environment is currently experiencing a significant shift due to the incorporation of networked devices in the era of the IoT. The incorporation of the IoT into the healthcare industry presents significant potential for enhancing the effectiveness, safety, and quality of healthcare services, in addition to offering exciting technical, economic, and societal opportunities. However, the incorporation of these systems inherently introduces security vulnerabilities, particularly the possibility of a data breach caused by the existence of malicious software intended to steal user login credentials. In addition, the possibility of the linked devices being vulnerable raises apprehensions around the potential disclosure of confidential patient information in the event of a security breach. The need of security has been more pronounced in the contemporary technological environment as a result of the extensive prevalence of IoT entities across diverse sectors. This includes the healthcare industry, which significantly depends on IoT-based solutions. Gordana et al, examine the methodology for anonymizing sensitive health data exchanged inside the IoT ecosystem using a wireless communication system. The algorithm employed in this system effectively preserves user privacy by implementing measures to shield sensitive records from unauthorized exposure. Consequently, it successfully upholds the principles of security and privacy during online user interactions. In addition, the strategy that was adopted incorporated a robust encryption technique, thereby enabling the safeguarding of confidential health data. In addition, an assessment of the anonymity feature of the methodology has been conducted using algebraic functions. The study's findings demonstrate that the utilization of the anonymization strategy successfully enhances the security features of the IoT system, specifically within hospital communication networks.

In the realm of the Home Area Network (HAN), sensors that possess IoT functionalities offer a reliable method for exchanging data securely, hence safeguarding the

integrity of this data. The incorporation of sensors and the exchange of energy measurements and data inside the smart grid offer a fresh outlook on energy management. The main aim of the study done was to examine the secure transmission of data within a HAN and to guarantee the safeguarding of client data privacy during important and time-sensitive operations. The data were effectively sent in real-time with little latency in transmission. The devices were subjected to routine examinations in order to verify their effectiveness in delivering critical services that save lives and are time-sensitive. The main emphasis of this article is on the transmission of machine-to-machine data and the transportation of packets within the framework of the IoT. The technology enabled the immediate retrieval of user power usage data in personalized electronic devices, as well as via cloud-based systems. This research endeavor demonstrated the essential requirements for constructing an economically viable HAN for the IoT that is interconnected with a smart grid, with a specific emphasis on energy-conscious routing. The integration of sensors and a control gateway inside a clearly delineated boundary proved to be advantageous in the endeavor to conserve energy during the processing and transmission of data in the sophisticated design blueprint. The assessment of the data flow pattern and packet delivery rate was performed by employing a combination of simulated and actual data acquired from sensors and concentrators. The collected data and flow patterns were assessed through the utilization of MATLAB and a network simulator. The deployment of the IoT-HAN system shown significant benefits in enabling secure data transmission between networked devices within the HAN. In their study, introduced a prototype called Future Spaces, which encompasses both hardware and software components. This prototype offers a high level of control over connectivity inside the Internet of Things (IoT) framework. The presented prototype facilitates the efficient and reliable administration of intelligent residential dwellings. The use of specialized network segments, utilizing home routers equipped with SDN capabilities and the virtualization of network services in cloud settings, has resulted in improved networking security and automation. The disturbance impeded users' ability to discover, manage, and distribute interconnected resources across several domains, while also seamlessly responding to different usage configurations.

The primary objective of this study is to investigate the many obstacles and potential opportunities related to a certain phenomenon. The IoT facilitates the management and monitoring of the digital realm. The IoT is a cutting-edge technical development that enables the monitoring of critical data. The IoT has emerged as a feasible approach for mitigating complexity and augmenting system efficiency in the realms of transportation, healthcare, and cyber systems. Pervasive computing plays a crucial role in enabling the IoT to efficiently handle data and offer the necessary graphical user interface. The retrieval of data from any point on the world at any given time is made possible through the utilization of cloud computing, a computer system that enhances access to information. Classifies several studies based on the landscape of data security. The main focus of the studies highlighted in this context revolves around the topic of data privacy. Numerous academic studies have conducted analyses on the subjects of data sharing and data confidentiality. In the foreseeable future, it is plausible that there will be the possibility of encountering unresolved complexities with the examination of data security inside the framework of the IoT. The domain of IoT security continues to present substantial prospects for further progress. Given the abundance of ongoing studies and existing obstacles, it is imperative for researchers to allocate their attention strategically in this particular domain. There are a number of current challenges pertaining to the security of the IoT that can be recognized. The scalability of blockchain technology is notably limited in situations where a substantial quantity of servers are involved. There are several highly effective strategies available for node replacement, and the utilization of different resources has become a widely accepted method for tackling this issue. Utilizing machine learning

methodologies, particularly AI and deep learning, to augment the efficacy of fog level improvement.

The main aim of fog sharing is to protect the computational capacities of fog-cloud systems. The prospective implementation of this approach may be viewed as a cause for optimism. The establishment of secure connections between various networks continues to require the utilization of end-to-end encryption methods and resilient shielding protocols. To successfully counteract hostile incursions, it is crucial for edge devices to possess a substantial degree of security and cognitive capabilities. The rapid expansion of IoT deployment across various industries has led to an increased focus on concerns regarding security. The IoT is presently in its early stages, mostly due to the significant research efforts conducted in recent years. The main impediment to the expansion of the IoT is the security domain, which gives birth to a multitude of challenges. Smart systems demonstrate the potential to effectively tackle many challenges faced in the industrial domain, although they do confront certain hindrances when it comes to seamlessly integrating with IoT and wireless sensors within the framework of Industry 4.0. Businesses and manufacturers face difficulties in effectively handling the growing volume of data that is being generated. The incorporation of artificial intelligence algorithms is crucial for the management of big data and the augmentation of system and device intelligence. Algorithms are utilized in order to process data across different time spans. The observed increase in the domain of security breaches and vulnerabilities in the IoT can be attributed to several factors. Firstly, there has been a notable growth in consumer and company awareness regarding these issues. Additionally, governmental and industrial entities have taken steps to address this concern by implementing labelling and certification programmes. Lastly, the costs associated with managing breaches in terms of public relations and reputation have also played a significant role in driving this rise.

Conclusion:

The limited length of the user's input precludes the possibility of rewriting it in an academic manner. The prioritization of efforts towards increasing system security is of utmost importance for enterprises, given the widespread use of the IoT. The existence of vulnerabilities within a system carries the risk of system failure or cyberattack, leading to substantial consequences on a wide-ranging level. The domain of IoT security covers a wide array of techniques and methods designed to protect against potential cyber threats that specifically exploit the weaknesses of interconnected IoT devices. Currently, IoT security teams are primarily focused on addressing many challenges, which encompass but are not limited to inventory management, operational issues, device diversity, effective management techniques, data traffic management, and the persistent threat landscape. This research investigates the multifaceted components of data security within the context of network security, placing specific emphasis on the circumstances, implementations, and obstacles linked to this domain. The analysis mostly relies on preexisting research published on security concerns related to the IoT. A grand total of 510 items were identified by employing the aforementioned keywords. The presence of duplication led to the removal of 40 entries. Consequently, there was a decline observed in the overall quantity of articles, which amounted to 450. The objects undergo inspection and filtration according to predetermined criteria for inclusion and rejection. As a result, a comprehensive analysis was conducted using a total of 20 research that satisfied the predetermined criteria. These studies were selected from the years 2012 to 2022. Based on empirical evidence, it has been observed that the IoT sector has been proactively addressing security concerns over a prolonged duration through the deployment of IoT security solutions aimed at safeguarding systems and devices against potential intrusions and compromises.

The IoT frequently offers crucial services for the creation of applications, encompassing data collection, management, as well as device and data security. IoT devices or gadgets participate in interactions and computational processes in order to augment security and improve the overall quality of life. The IoT possesses the capacity to facilitate the automation of inventories, enable real-time monitoring of items, and provide support for the administration of information and the status of diverse entities. In order to facilitate the transfer of a substantial amount of data among network devices, it is imperative to develop a comprehensive security architecture that guarantees the maintenance of data integrity, confidentiality, authentication, and authorization. A multitude of research efforts have been devoted to investigating various approaches with the objective of improving the verification capabilities of a broad spectrum of systems, including wireless systems. The field of IoT security continues to present substantial prospects for further development. Given the abundance of ongoing studies and the related complexities, it is imperative for researchers to allocate their attention to this specific topic. The scalability of blockchain is considerably limited when there is a substantial number of servers involved. There are currently highly effective strategies available for the replacement of nodes, and the utilization of many resources has become a commonly accepted method for tackling this problem. In the future, upcoming endeavors may focus on a wide array of technologies, such as machine learning, artificial intelligence, blockchain, and various others.

References:

[1] A. A. G.-E. Ahmed and A. A. G.-E. Ahmed, "Benefits and Challenges of Internet of Things for Telecommunication Networks," Telecommun. Networks - Trends Dev., Feb. 2019, doi: 10.5772/INTECHOPEN.81891.

[2] F. T. Jaigirdar, B. Tan, C. Rudolph, and C. Bain, "Security-Aware Provenance for Transparency in IoT Data Propagation," IEEE Access, vol. 11, pp. 55677–55691, 2023, doi: 10.1109/ACCESS.2023.3280928.

[3] H. Ning, H. Liu, and L. T. Yang, "Cyberentity security in the internet of things," Computer (Long. Beach. Calif)., vol. 46, no. 4, pp. 46–53, 2013, doi: 10.1109/MC.2013.74.

[4] A. Bogdanov et al., "PRESENT: An ultra-lightweight block cipher," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 4727 LNCS, pp. 450–466, 2007, doi: 10.1007/978-3-540-74735-2_31.

[5] F. Thabit, O. Can, A. O. Aljahdali, G. H. Al-Gaphari, and H. A. Alkhzaimi, "Cryptography Algorithms for Enhancing IoT Security," Internet of Things (Netherlands), vol. 22, Jul. 2023, doi: 10.1016/j.iot.2023.100759.

[6] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of Things security: A survey," J. Netw. Comput. Appl., vol. 88, pp. 10–28, Jun. 2017, doi: 10.1016/J.JNCA.2017.04.002.

[7] U. Farooq, N. Tariq, M. Asim, T. Baker, and A. Al-Shamma'a, "Machine learning and the Internet of Things security: Solutions and open challenges," J. Parallel Distrib. Comput., vol. 162, pp. 89–104, Apr. 2022, doi: 10.1016/J.JPDC.2022.01.015.

[8] P. Peris-Lopez, Ed., "2015 International Workshop on Secure Internet of Things, SIoT 2015, Vienna, Austria, September 21-25, 2015," SIoT, 2015, Accessed: Oct. 09, 2023. [Online]. Available: http://dblp.uni-trier.de/db/conf/siot/siot2015.html

[9] W. Detres, M. M. Chowdhury, and N. Rifat, "IoT Security and Privacy," IEEE Int. Conf. Electro Inf. Technol., vol. 2022-May, pp. 498–503, 2022, doi: 10.1109/EIT53891.2022.9813933.

[10] E. Farooq, S. A. Khan, and W. H. Butt, "Covert network analysis to detect key players using correlation and social network analysis," ACM Int. Conf. Proceeding Ser., Mar.

2017, doi: 10.1145/3018896.3025142.

[11] P. Mugariri, H. Abdullah, M. García-Torres, B. D. Parameshchari, and K. N. Abdul Sattar, "Promoting Information Privacy Protection Awareness for Internet of Things (IoT)," Mob. Inf. Syst., vol. 2022, 2022, doi: 10.1155/2022/4247651.

[12] S. Volpert, P. Eichhammer, F. Held, T. Huffert, H. P. Reiser, and J. Domaschka, "The view on systems monitoring and its requirements from future Cloud-to-Thing applications and infrastructures," Futur. Gener. Comput. Syst., vol. 141, pp. 243–257, Apr. 2023, doi: 10.1016/J.FUTURE.2022.11.024.

[13] A. Boudguiga, A. Olivereau, and N. Oualha, "Server assisted key establishment for WSN: A mikey-ticket approach," Proc. - 12th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust. 2013, pp. 94–101, 2013, doi: 10.1109/TRUSTCOM.2013.16.

[14] H. Zhou, G. Yang, Y. Xiang, Y. Bai, and W. Wang, "A Lightweight Matrix Factorization for Recommendation With Local Differential Privacy in Big Data," IEEE Trans. Big Data, vol. 9, no. 1, pp. 160–173, Feb. 2023, doi: 10.1109/TBDATA.2021.3139125.

[15] A. Nakamura, K. Naito, and T. Yamazato, "Distributed processing framework for cooperative service among edge devices," Dig. Tech. Pap. - IEEE Int. Conf. Consum. Electron., vol. 2023-January, 2023, doi: 10.1109/ICCE56470.2023.10043588.

[16] F. V. Meca, J. H. Ziegeldorf, P. M. Sanchez, O. G. Morchon, S. S. Kumar, and S. L. Keoh, "HIP Security architecture for the IP-based internet of things," Proc. - 27th Int. Conf. Adv. Inf. Netw. Appl. Work. WAINA 2013, pp. 1331–1336, 2013, doi: 10.1109/WAINA.2013.158.

[17] D. Liu, P. Ning, and L. I. Rongfang, "Establishing pairwise keys in distributed sensor networks," ACM Trans. Inf. Syst. Secur., vol. 8, no. 1, pp. 41–77, Feb. 2005, doi: 10.1145/1053283.1053287.

[18] T. Ito, H. Ohta, N. Matsuda, and T. Yoneda, "A key pre-distribution scheme for secure sensor networks using probability density function of node deployment," SASN'05 - Proc. 2005 ACM Work. Secur. Ad Hoc Sens. Networks, vol. 2005, pp. 69–75, 2005, doi: 10.1145/1102219.1102233.

[19] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," Proc. ACM Conf. Comput. Commun. Secur., pp. 41–47, 2002, doi: 10.1145/586110.586117.

[20] G. De Meulenaer, F. Gosset, F. X. Standaert, and O. Pereira, "On the energy cost of communication and cryptography in wireless sensor networks," Proc. - 4th IEEE Int. Conf. Wirel. Mob. Comput. Netw. Commun. WiMob 2008, pp. 580–585, 2008, doi: 10.1109/WIMOB.2008.16.

[21] W. Du, J. Deng, and Y. S. Han, "A key predistribution scheme for sensor networks using deployment knowledge," IEEE Trans. Dependable Secur. Comput., vol. 3, no. 1, pp. 62–77, 2006, doi: 10.1109/TDSC.2006.2.

[22] E. Rescorla, "Diffie-Hellman Key Agreement Method," Jun. 1999, doi: 10.17487/RFC2631.

[23] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges," Wirel. Networks, vol. 20, no. 8, pp. 2481–2501, Oct. 2014, doi: 10.1007/S11276-014-0761-7.

[24] R. Hummen, J. H. Ziegeldorf, H. Shafagh, S. Raza, and K. Wehrle, "Towards viable certificate-based authentication for the Internet of Things," HotWiSec 2013 - Proc. 2013 ACM Work. Hot Top. Wirel. Netw. Secur. Priv., pp. 37–41, 2013, doi: 10.1145/2463183.2463193.

[25] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of things: The road ahead," Comput. Networks, vol. 76, pp. 146–164, Jan. 2015, doi: 10.1016/J.COMNET.2014.11.008.

[26] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Comput. Networks, vol. 57, no. 10, pp. 2266–2279, Jul. 2013, doi: 10.1016/J.COMNET.2012.12.018.

[27] K. T. Nguyen, M. Laurent, and N. Oualha, "Survey on secure communication protocols for the Internet of Things," Ad Hoc Networks, vol. 32, pp. 17–31, Sep. 2015, doi: 10.1016/J.ADHOC.2015.01.006.

[28] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," Ad Hoc Networks, vol. 10, no. 7, pp. 1497–1516, 2012, doi: 10.1016/J.ADHOC.2012.02.016.

[29] S. A. A. Shukor, M. Q. Aminuddin, and E. J. Rushforth, "Managing huge point cloud data through geometrical-based registration," ACM Int. Conf. Proceeding Ser., Mar. 2017, doi: 10.1145/3018896.3056783.

[30] M. A. Taiye, S. S. Kamaruddin, and F. K. Ahmad, "Combined WSD algorithms with LSA to identify semantic similarity in unstructured textual data," ACM Int. Conf. Proceeding Ser., Mar. 2017, doi: 10.1145/3018896.3056785.

[31] A. Harit, A. Ezzati, and R. Elharti, "Internet of things security: Challenges and perspectives," ACM Int. Conf. Proceeding Ser., Mar. 2017, doi: 10.1145/3018896.3056784.

[32] M. Javaid and I. H. Khan, "Internet of Things (IoT) enabled healthcare helps to take the challenges of COVID-19 Pandemic," J. Oral Biol. Craniofacial Res., vol. 11, no. 2, pp. 209–214, Apr. 2021, doi: 10.1016/J.JOBCR.2021.01.015.

[33] A. Ghasempour, "Internet of things in smart grid: Architecture, applications, services, key technologies, and challenges," Inventions, vol. 4, no. 1, Mar. 2019, doi: 10.3390/INVENTIONS4010022.

[34] P. Radanliev and D. De Roure, "Alternative mental health therapies in prolonged lockdowns: narratives from Covid-19," Health Technol. (Berl)., vol. 11, no. 5, pp. 1101–1107, Sep. 2021, doi: 10.1007/S12553-021-00581-3.

[35] S. Madakam, R. Ramaswamy, and S. Tripathi, "Internet of Things (IoT): A Literature Review," J. Comput. Commun., vol. 03, no. 05, pp. 164–173, 2015, doi: 10.4236/JCC.2015.35021.

[36] J. Pike, T. Bogich, S. Elwood, D. C. Finnoff, and P. Daszak, "Economic optimization of a global strategy to address the pandemic threat," Proc. Natl. Acad. Sci. U. S. A., vol. 111, no. 52, pp. 18519–18523, Dec. 2014, doi: 10.1073/PNAS.1412661112.

[37] T. Mohammed, C. Jean-Yves, B. Peter, and R. Christophe, "Petrogenesis of the post-collisional Bled M'Dena volcanic ring complex in Reguibat Rise (western Eglab shield, Algeria)," J. African Earth Sci., vol. 166, Jun. 2020, doi: 10.1016/J.JAFREARSCI.2015.04.003.

[38] P. J. Ryan and R. B. Watson, "Research challenges for the internet of things: What role can or play?," Systems, vol. 5, no. 1, Mar. 2017, doi: 10.3390/SYSTEMS5010024.

[39] E. A. Kosmatos, N. D. Tselikas, and A. C. Boucouvalas, "Integrating RFIDs and Smart Objects into a UnifiedInternet of Things Architecture," Adv. Internet Things, vol. 01, no. 01, pp. 5–12, 2011, doi: 10.4236/AIT.2011.11002.

[40] P. Radanliev and D. De Roure, "Epistemological and bibliometric analysis of ethics and shared responsibility—health policy and IoT systems," Sustain., vol. 13, no. 15, Aug. 2021, doi: 10.3390/SU13158355.

[41] S. Rivard and S. L. Huff, "Factors of Success for End-User Computing," Commun.

ACM, vol. 31, no. 5, pp. 552–561, May 1988, doi: 10.1145/42411.42418.

[42] B. R. Hayes-Gill, "Monica Healthcare: From the research laboratory to commercial reality—A real-life case study," Healthc. Technol. Lett., vol. 8, no. 1, pp. 1–10, Feb. 2021, doi: 10.1049/HTL2.12004.

[43] S. A. Kumar, T. Vealey, and H. Srivastava, "Security in internet of things: Challenges, solutions and future directions," Proc. Annu. Hawaii Int. Conf. Syst. Sci., vol. 2016-March, pp. 5772–5781, Mar. 2016, doi: 10.1109/HICSS.2016.714.

[44] W. V. B. de Souza et al., "Using Crowdstorm to Prospect Innovations in Federal Institutions of Education in Brazil to Reduce Its Consumption of Electric Energy," 49th Hawaii Int. Conf. Syst. Sci. (HICSS 2016), pp. 2819–2828, 2016, doi: 10.1109/HICSS.2016.353.

[45] C. Dobre, L. Bajenaru, I. A. Marinescu, and M. Tomescu, "Improving the quality of life for older people: From smart sensors to distributed platforms," Proc. - 2019 22nd Int. Conf. Control Syst. Comput. Sci. CSCS 2019, pp. 636–642, May 2019, doi: 10.1109/CSCS.2019.00115.