International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 11 Issue: 09 | Sep 2024 www.irjet.net p-ISSN: 2395-0072

SECURITY IMPLICATION OF INTERNET OF THING (IOT) DEVICES

N Chaitanya[1]

[1]*Wipro*

Abstract - *The internet of factors (IoT) has basically transformed connectivity, linking numerous embedded gadgets with awesome identifiers and embedded software for seamless communique. however, the huge adoption of IoT gadgets brings forth a myriad of protection challenges. This survey paper delves into the unique security challenges inherent in cutting-edge IoT requirements and protocols. thru radical research, this looks at identifies the risks related to the present IoT landscape, explores rising security protocols, and highlights latest protection initiatives aimed toward bolstering IoT structures. furthermore, it offers an up to date evaluate of IoT structure, scrutinizing protocols and standards poised to form the next era of IoT structures. A comparative analysis of protection protocols, standards, and proposed security models is provided, consistent with the evolving protection desires of IoT. The examine underscores the need for standardization at communique and information audit tiers to mitigate threats to hardware, software, and statistics integrity. additionally, it advocates for the development of protocols capable of effectively addressing more than one threat vectors. with the aid of synthesizing the modern-day traits in safety studies, this paper gives treasured insights for reinforcing IoT protection. The study's findings are expected to advantage the broader IoT studies community via promoting the combination of exceptional security practices into IoT-based gadgets*

Key Words*: *Protocols, Link embedded device, Enhanced IoT security

1.INTRODUCTION

The field of networking has experienced a major technical revolution in recent years., particularly with the advent of automation. This trend has been further augmented by the emergence of Internet of Things (IoT) technology, which plays a pivotal role in shaping this evolving landscape. The Internet of Things, as defined in literature [1], encompasses a network of interconnected devices dedicated to tasks such as data transmission, reception, and processing. Initially confined to over time, the Internet of Things (IoT) has broadened to include Industrial IoT frameworks, which are local physical devices connected to the internet for real-time data processing [2]. IoT research shows how pervasive it is in several industries, including corporate analytics, healthcare, industrial settings, and education [3, 4]. In 2019 and beyond, IoT once operated within smaller network spaces, has now transitioned to encompass wide area networks. Alongside this expansion, however, comes an associated increase in security risks, owing to the projected proliferation of IoT devices within diverse environments.

1.1 Research Challenges in IoT Security

This research project's main goal is to investigate the most recent security paradigms in the Internet of Things domain. Apart from this main goal, there are also supporting goals such as identifying and characterizing current IoT security threats. However, it is essential to overcome the current research problems in the IoT ecosystem before beginning this exploration:

- Heterogeneity Issue: The diverse range of devices, protocols, and communication mechanisms within IoT ecosystems poses a significant challenge in terms of interoperability and standardization [16].

- Inter-connectivity: The seamless interconnection of numerous devices in IoT networks raises concerns regarding data privacy, integrity, and secure communication channels [17].

- Ubiquitous Nature: The pervasive deployment of IoT devices across various domains introduces complexities in managing and securing these distributed systems effectively [18].

- Security Standards Issue: The absence of comprehensive security standards tailored specifically for IoT exacerbates vulnerabilities and undermines overall system resilience [19]. Emerging technical fields like software-enabled networking, machine learning, and artificial intelligence with cluster□based fuzzy logic modules have become crucial areas of study for integrating with the Internet of Things [20]. The introduction of ultra-lightweight protocols, which are strategically used to ease core operations and handle security concerns, is a major achievement in the Internet of Things .

1.2 Research contribution

Research endeavors focusing on IoT security challenges encompass a broad spectrum and continually evolve, with new vulnerabilities surfacing regularly. Presently, discussions around IoT security predominantly revolve around access control methodologies, encryption techniques for temporary periods, security fixes unique to hardware, and safeguards against SQL-based input assaults . Thus, our

research endeavors to elucidate the dynamic security landscape of IoT by delineating pertinent security issues, providing precise definitions, classification, and exploring contemporary solutions to mitigate these challenges. The motivation behind this work lies in exploring the security concerns associated with IoT-based devices across various IoT applications. To comprehend the security aspect of IoT, it is essential to gain prior knowledge about the underlying infrastructure. Hence, we delve into discussing IoT architecture and carry out a comparison study of the protocols and standards that are frequently employed in IoT settings. Our second study contribution is an in-depth analysis of current developments in Internet of Things security. aimed at informing the development of robust IoT security frameworks. We thoroughly examine the most common dangers found in IoT systems today in this survey, as well as the most recent security strategies that have been suggested for the Internet of Things in the last few years. Establishing security solutions is the goal that are compliant with the security standards of the Internet of Things (IoT) and cover elements like trust management, confidentiality, integrity, and authenticity [16]. The identification and comparative analysis of widely used protocols and standards in the Internet of Things constitute our third research contribution. We discuss the most recent advancements and standardization techniques applied to IoT [17], categorize security vulnerabilities in IoT according to the degree to which they affect the environment as a whole, and suggest relevant fixes. Studies show that new security design models and current encryption methods are frequently used in IoT security solutions. The integrity of communication and trust have been cited as major security concerns. Furthermore, it has been noted that connecting IoT with other networks, including Software-Defined Networking (SDN), exacerbates IoT security concerns [18, 19]. Additionally, we acknowledge the need for manufacturing-level standardization, which highlights weaknesses at the hardware and software levels [20]. Our experiments further demonstrate the necessity of protocols that can handle several attack vectors.

The results of this research project are expected to support the inclusion of the most appropriate and secure features in IoT-based devices, which will be advantageous to the IoT research community. This paper is organized as follows: The study is briefly introduced in Section 1. A survey of recent research on IoT security advancements is given in Section 2. The architecture of the Internet of Things is covered in Section 3, along with popular IoT protocols and standards. IoT security trends are covered in detail in Section 4. While Section 6 wraps up the thorough survey work, Section 5 gives the findings and analysis of the complete research project.

2. LITERATURE REVIEW

A Review on Security Challenges in Internet of Things (IoT): In this extensive review, Researcher and Scholar meticulously scrutinize a plethora of scholarly works addressing the multifaceted security challenges embedded within the Internet of Things (IoT). Synthesizing insights from seminal research, the survey not only highlights prevalent vulnerabilities but also dissects diverse threat vectors and evolving attack scenarios across a spectrum of IoT applications. By providing a comprehensive overview, this survey contributes to a nuanced understanding of the dynamic and ever-evolving threat landscape surrounding IoT devices, serving as a foundational resource for researchers, policymakers, and industry practitioners.

Security Issues in the Internet of Things (IoT): A Comprehensive Study: Scientist and Expert navigate the intricacies of current trends shaping security protocols within the IoT ecosystem. Focusing keenly on device authentication, data encryption, and firmware updates, the survey meticulously identifies recent advancements while critically assessing existing practices. This comprehensive analysis not only lays bare the vulnerabilities but also proposes tangible enhancements to fortify the security posture of IoT devices. The survey stands as a technical compass guiding developers, security professionals, and stakeholders through the rapidly evolving landscape of securing IoT devices.

A survey on security in internet of things with a focus on the impact of emerging technologies: Authority and Regulation embark on a meticulous comparative analysis of regulatory frameworks governing IoT security. Traversing the intricate web of governmental and industry standards, the survey evaluates the effectiveness of these frameworks in addressing nuanced security concerns within the diverse IoT landscape. This literature review offers valuable insights into the regulatory measures necessary for mitigating security risks, shaping policy decisions, and ensuring the trustworthiness of IoT environments as they integrate into our daily lives.

Security in Internet of Things: Issues, Challenges, and Solutions: Investigator and Analyst conduct a forensic exploration of real-world cybersecurity incidents, immersing themselves in the intricacies of breaches involving IoT devices. Through in-depth case studies, the survey meticulously analyzes the root causes, consequences, and the invaluable lessons learned from these incidents. By distilling actionable knowledge, this survey serves as a vital repository of insights for both researchers and practitioners, providing a roadmap for fortifying the resilience of IoT ecosystems against evolving cyber threats.

A decade of research on patterns and architectures for IoT security: Engineer and Industrialist direct their focus towards the unique security challenges inherent in Industrial IoT (IIoT) applications. The survey meticulously reviews existing frameworks tailored for the industrial sector, addressing critical aspects such as infrastructure protection and secure communication. By identifying best

practices and highlighting gaps in security measures, this review becomes an indispensable resource for securing IoT deployments, contributing to the safety and reliability of industrial processes.

IoT Security: Ongoing Challenges and Research Opportunities: Technologist and Innovator embark on an exploration of cutting-edge solutions and technologies designed to fortify IoT security. The survey reviews recent advancements in blockchain, artificial intelligence, and machine learning applied to IoT security. By assessing the potential of these technologies to address current vulnerabilities, this survey provides a forward-looking perspective, guiding the evolution of secure IoT ecosystems into the future. Wireless networking equipped with embedded networking capability represents the prevailing industrial trend worldwide, with IoT being one of the primary beneficiaries of this networking domain. Over recent years, IoT has witnessed significant development through the integration of Cloud services, offering Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS).

The commercial sectors of IoT have experienced substantial growth in the market, fueled by escalating demands for smart systems boasting rich features and convenient services. Smart systems, including Smart Home appliances, AI-based devices, home automation systems, smart vehicles, and smart laboratories, offer enhanced convenience but also introduce heightened dependence, leading to elevated risks. Figure 1, based on statistics from Statista , illustrates the projected surge in IoT devices in the near future. Technical reports suggest that IoT devices have become prime targets for intrusion activities by hackers, owing to the prevalence of lightweight protocols , coupled with the accessibility of entities constituting these devices to the server . These factors present challenges to technology as there is inadequate addressing of security concerns for the latter. It is evident that the threat structure is not confined to a specific layer in IoT architecture . Traditional network security practices integrated into IoT have often resulted in performance degradation of IoT systems. It comprises a compilation of recent innovative models proposed in response to advanced threat reports in IoT. We delineate the security parameters, for which certain research works offer security models in contrast to conventional security models. Historically, challenges in the IoT ecosystem have included inter-compatibility among security tools deployed for IoT devices because of variations in implementation methods and policies, in addition to the absence of device algorithms with minimal processing power . In order to get beyond traditional security problems, recent research has suggested creative ways that make use of hardware-based techniques and a variety of encryption techniques . To assure valid authentication and solve trust-centric threat models, Xin Zhang and Fengtong Wen, for example, present a novel anonymous user Wireless Sensor Network (WSN) authentication technique for the Internet of Things (IoT). This method incorporates UDS (user-device-server) and USD (user-server-device) algorithmic models. But the reach of this approach is narrow; it offers security solutions just for low-weight sensor devices against common physical and network‐based threats. Furthermore, Mohammad Dahman Alshehri and Farookh Khadeer Hussain propose a cluster-based fuzzy logic implementation model and a secure messaging paradigm between IoT nodes, utilizing encrypted communication to mitigate threats such as Port Scanning. While effective in detecting malicious IoT nodes, this model does not adequately address data audit attack vulnerabilities and lacks performance analysis concerning communication and computation costs. Priyanka et al. [13] introduce a multi-stage security model employing Elliptical Curve Cryptography (ECC) and fully homomorphic encryption (FHE) to ensure data integrity in the IoT environment with reduced computational overheads. Nonetheless, concerns remain regarding increased data overheads and computational costs associated with this model. Munkenyi Mukhandi and colleagues [5] present a new security approach for robotic communication in the context of Industrial IoT. They do this by utilizing the Robot Operating System and MQTT protocols, as well as data encryption and authentication techniques. There are differences between performance measures and cryptographic functions, even though they are effective in safeguarding communication routes. Deep learning and machine learning have made significant inroads in the IoT environment, with products like Alexa and Echo relying on voice commands for real‐time actions. However, issues such as data packet leaks have prompted the development of voice recognition applications, such as the one proposed by Pooja Shree Singh and Vineet Khanna, based on Mel-frequency cepstral coefficients (MFCC) for user identification and authentication. Nonetheless, dependency on hardware architecture remains a challenge. Access control-related issues have plagued IoT since its inception. To address this, Michail Sidorov et al. [10] propose a secure ultra-lightweight RFID protocol for integration into supply chain management systems, leveraging permissioned blockchain networks and encryption at various access levels. While promising, concerns remain regarding setup costs. Chen et al. present a novel low-scale Denial-of‐Service attack detection approach using Trust evaluation with Hilbert-Huang Transformation in Zigbee Wireless Sensor Networks (WSN) to mitigate security threats to low-energy devices. This approach offers scalable architecture covering both cloud and edge computing IoT devices but faces challenges related to storage overheads.

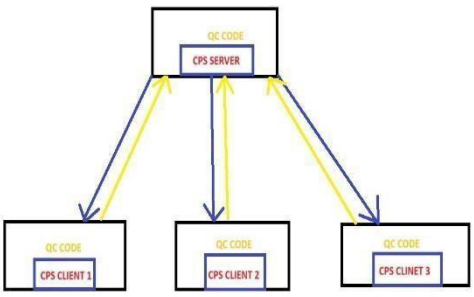
3. PROPOSED ARCHITECTURE

The Internet of Things encompasses a diverse array of industries and applications, ranging from small, single‐purpose devices to extensive deployments spanning various embedded technologies and cloud systems, all

interconnected in real-time. As previously mentioned, IoT operations revolve around three key functions: transmitting, retrieving, and processing data. Essentially, IoT technology facilitates the exchange of data among heterogeneous devices, enabling continuous information streaming between interconnected devices.

3.1 Layered architecture

The architecture used by the Internet of Things is multi‐layer and multi-plane. The Device Management part, the Application Interface section, and the Communication plane are the three primary components of this design. Devices communicate with the underlying architecture in the Application Interface Layer via embedded interface modules, which are essential parts of this architectural segment and include the Arduino IDE, Raspberry Pi, sensors, actuators, and more. By determining the source and destination of data, the Device Management Plane manages the input/output capabilities of devices. An aggregator, for example, functions as a centralized unit in charge of combining data obtained from several devices. As an intermediary layer between switches and other network components, the communication layer establishes standards and communication protocols for Internet of Things network traffic. In order to handle network traffic throughout the entire system, this layer consists of protocol stacks that implement the most recent protocols and standards. Newer communication protocols with better congestion control capabilities, a focus on energy saving, and improved Quality of Service (QoS) features are employed in embedded IoT contexts.



3.2 Communication protocols

Communication among IoT devices relies on standard protocols such as MQTT (Message Queueing Telemetry Transport), AMQP, DDS, ZigBee, and LoRaWAN , among others. These protocols establish standardized rules for facilitating information sharing within the IoT environment, ensuring compatibility and ease of initialization. Bluetooth Low Energy (BLE) Protocol: Widely utilized in the IoT landscape, BLE stands out for its low energy consumption, making it suitable for energy-efficient devices. Based on Generic Attributes, BLE operates through services and characteristics. Message Queueing Telemetry Transport (MQTT) Protocol: Specifically designed for lightweight IoT devices, MQTT facilitates data transmission and reception between sensor nodes. Its operation revolves around three key components: Publisher, Broker, and Subscriber, where the Broker serves as the intermediary server analyzing transmitted data. Advanced Message Queueing Protocol (AMQP) : Known for its efficiency, portability, multi- channel support, and security features, AMQP ensures authentication through SASL or TLS, making it suitable for multi-client environments. Constrained Application Protocol (CoAP) : Designed for constrained environments, CoAP operates based on REST API structure, catering to smart system applications. Notable characteristics include congestion control and cross-protocol integration. Data Distribution Service (DDS) Protocol: Developed for Machine-to-Machine (M2M) Communication in IoT, DDS facilitates data exchange through a publish-subscribe method, employing a broker-less architecture and multicasting to ensure high-quality QoS across devices. While these protocols enhance scalability, performance, and applicability in IoT ecosystems, they may introduce security vulnerabilities, a topic explored further in subsequent sections of this paper. These IoT protocols have laid the groundwork for seamless integration of IoT with existing wireless technologies such as cloud computing, edge computing, and lightweight embedded systems. Despite advancements in scalability and performance, security concerns persist and will be addressed in subsequent sections.

4. METHODLOGY

• Identify Assets and Threats: Identify the assets (e.g., IoT devices, data) associated with the IoT ecosystem. Identify potential threats and vulnerabilities that could compromise the security of these assets. • Assess Vulnerabilities: Evaluate the vulnerabilities present in IoT devices and the surrounding ecosystem. Assign a vulnerability score (VS) to each identified vulnerability using a scoring system (e.g., 1 to 10 scale).

• Estimate Threat Probability: Estimate the likelihood of each identified threat occurring. Assign a threat probability score (TPS) to each threat using a scoring system (e.g., low, medium, high).

• Calculate Risk Score: Calculate the risk score (RS) for each vulnerability by multiplying the vulnerability score (VS) with the threat probability score (TPS).

$$RS = VS * TPS$$

• Prioritize Risks: Prioritize risks based on their calculated risk scores. Higher risk scores indicate greater potential impact and likelihood of occurrence.

Example:

Consider a simplified scenario with three vulnerabilities (V1, V2, V3) identified in IoT devices, each with its corresponding vulnerability score (VS) and threat probability score (TPS): Consider a simplified scenario with three vulnerabilities (V1, V2, V3) identified in IoT devices, each with its corresponding vulnerability score (VS) and threat probability score (TPS):

Vulnerability	Vulnerability Score (VS)	Threat Probability Score (TPS)	Risk Score (RS)
V1	8	High	8*High=8
V2	5	Medium	5*Medium=5
V3	3	Low	3*Low=3

Table1: Risk Score Assessment

Based on the calculated risk scores, vulnerabilities can be prioritized for mitigation efforts. In this example, V1 poses the highest risk, followed by V2 and V3.

4.1 Security challenges

The analysis concerning IoT protocols and standards reveals significant vulnerabilities, particularly in access requests, identification of third- party involvement, and weak compliance with security management scalability. Current security challenges in IoT, aligned with conventional network architecture, include: Heterogeneous Device Configuration: Unlike conventional network devices, IoT devices interact with the physical world in diverse ways. This heterogeneity in IoT devices' operations can impact other networking components, necessitating consideration of IoT-specific privacy policies and cyber controls to address the ramifications on physical systems, thereby presenting a security issue.

Dispersive Network Update Policy: Managing IoT devices globally entails coordination through distributed servers, each governed by separate rule engines and security policies. Updating all devices uniformly poses challenges, including varying update rates, leaving behind non-updated devices during switchovers, or inadequately configured nodes due to the sheer volume of nodes requiring monitoring. Third-party intervention in support of updates can compromise access control, particularly for organizations with geographically dispersed locations, resulting in cost-prohibitive and time‐consuming issues.

Add-Ins Security Policy: IoT was not initially designed to incorporate robust security features. Consequently, additional plugins and security controls are appended to the layered IoT architecture to enhance security. Unlike traditional network paradigms, the effectiveness of these security characteristics depends on the additional resources' functionality within the IoT architecture, with client actions impacting the overall security effectiveness of IoT. Physical IoT Threats: Enterprise domains, network‐integrated healthcare systems, and industrial setups are all at serious risk from physical security concerns. Data audit features and communication channels are important security vectors. Communication channel concerns include trust management and authentication problems between stakeholders and network organizations, while security problems unique to data audits reveal weaknesses at the aggregator layer of IoT architecture and during large-scale data transfer. Physical threats also encompass manual or natural destruction of network components and malfunctioning of IoT equipment like robotics and sensors, potentially impacting physical entities within industrial systems.

4.2 Classifcation of attacks in IoT

Identifying possible risks in IoT design by analyzing target sets and behavior is essential to creating security solutions that work. Lately, a lot of for-profit companies have committed significant funds to safeguarding their Internet of Things networks. Two components can be used to classify IoT attacks: Protocol-Based Attacks: These attacks target embedded system forwarding channels and communication media by taking advantage of the inherent protocol-based structure of Internet of Things components.

This group is separated further into:

a) Attacks Based on Communication Protocols: These attacks, which include sniffing, flooding, and pre-shared key assaults, happen when nodes are transitioning.

b) Attacks Based on Network Protocols: These attacks, which include sniffer, wormhole, and selective forward assaults, aim to disrupt the process of establishing a connection.

4.3 Classifcation of IoT attacks based on active and passive forms

Understanding IoT attacks' effects on network security and performance requires dividing them into active and passive categories. Notably, security solutions designed for different types of active and passive assaults in the Internet of Things might have rather diverse effects on network speed. While defending against passive attacks usually entails monitoring techniques with relatively little impact on network performance, active attacks require responsive security systems to mitigate risks and maintain network performance. Attacks known as "traffic sniffing" entail the active collection of data in order to get vital system information for later attacks, such as botnet attacks. Sophisticated tools are used to examine data assets such usernames, passwords, raw data, authentication schemes, and device specifications. Many Internet of Things (IoT)

devices are weak points because they lack the intelligence to counteract such assaults.

Masquerade Attack: Through the use of a fictitious network ID, masquerade attacks aim to obtain unauthorized access to the data of the target node by circumventing official access identification procedures. Weak authorization processes put devices at risk because hackers can compromise security by using user credentials and stolen passwords to obtain access. Replay Attack: Replay attacks involve listening in on secure communication channels between Internet of Things devices or gateways, intercepting acknowledgments or parts of the connection establishment process, and then replaying messages falsely in order to control the behavior or results of the devices. This exploit interferes with regular device functions, which may allow attackers to access servers without authorization. Port Scanning: This technique looks for open or listening nodes, examines source and firewall packets, target ports, and target hosts' responses to SYN requests. Commonly used techniques like SYN scans use responses to infer port status while sending SYN packets to target nodes in order to partially establish connections. Hosts respond with SYN/ACK packets or RST packets, signaling open or closed ports, respectively, based on firewall regulations and port status.

4.4 Comparative analysis of IoT protocols

Modern IoT security solutions are more heavily weighted toward software-centric strategies than they are toward more conventional tool-centric ones. Modern security solutions highlight important security factors including authentication, trust, and communication channel integrity among IoT devices. Nonetheless, there are still issues with the IoT infrastructure as it relates to handling powerful devices and expanding entity variety. IoT integration with cutting-edge technologies such as Software-Defined Networking (SDN) presents new security challenges while also providing opportunity for enhanced scalability, node management, security policy, and reliability. Evaluating the different energy-efficiency and security properties of the protocols. Although there has been an improvement in performance, rule flows now contain vulnerabilities. For example, the CoAP protocol offers security during data transfer by supporting DTLS and IPSec; yet, it is still susceptible to load-based assaults, such DDoS and botnet attacks [64, 65]. In contrast, the MQTT protocol offers security through Transport Layer Security (TLS) or Secure Socket Layer (SSL) encryption; yet, it is susceptible to malicious node subscription attacks and botnet attacks. EnOcean employs a unique rolling code key encryption technique to protect nodes, however issues with code synchronization and key privacy persist. SigFOX's robust firewalls, hardware security modules, and public key infrastructure provide security benefits for dynamic IoT scenarios. Payload encryption is still problematic, though. Despite these issues, the low energy consumption of these protocols has the potential to improve network performance in dense IoT deployments.

5. RESULTS AND DISCUSSION

The comparison analysis's findings show that most of the attack surfaces seen in IoT environments are successfully addressed by protocol-based security solutions. Through the implementation of security safeguards at the Data Link and Transport layers, protocols like COAP and DDS provide strong defense against well-known threats like DDoS attacks and botnet incursions. For protocols such as SigFOX and EnOcean, novel strategies have been devised to counter new threats including asymmetric code definitions and vulnerabilities in payload encryption via specialized encryption methods. Additionally, lightweight protocols like BLE and MQTT have shown to be effective defenses against threats like man□in-the-middle and malicious node assaults. Furthermore, Physically Unclonable Function (PUF) protocols have been established to fight alterations made to IoT devices through physical attacks. These protocols provide distinctive authentication procedures based on PUFs to successfully combat risks emerging from physical attacks. They do this by mounting specially designed PUF chips on Internet of Things devices. To further address the confidentiality, integrity, authenticity, availability, and trust-based security requirements in IoT environments, new encryption techniques, machine learning approaches, blockchain technology, and socket programming have been incorporated into security models that have been developed based on these protocols and standards. Using a segmented approach to security management makes it easier to handle security measures and increases their efficacy. VI. FUTURE WORKS Homomorphic encryption is essential in IoT to address security concerns associated with sensitive data transmission and processing. It enables encrypted data to be manipulated and analyzed without decryption, preserving confidentiality throughout the process. This ensures that IoT systems can securely transmit, store, and process data without compromising privacy or integrity. IoT devices may function in areas that are intrinsically unsafe thanks to homomorphic encryption, which also protects private data from prospective hackers and unlawful access. Integrating homomorphic encryption into IoT systems involves a comprehensive approach. First, an appropriate algorithm is selected, considering computational efficiency and security. Robust key management practices are established for secure key distribution and rotation. IoT devices are equipped with encryption capabilities, ensuring data is encrypted before transmission. Secure communication protocols are employed for data transmission to cloud servers. Cloud servers are configured to support homomorphic operations, enabling secure data processing. Homomorphic computations, including addition and multiplication, are performed directly on encrypted data. Optimization techniques are applied to enhance performance. Finally, results are decrypted using authorized private keys, ensuring data confidentiality. This

seamless integration enhances IoT security, enabling secure data transmission, processing, and analysis in various applications.

6. CONCLUSION

This study has examined recently proposed models, protocols, and encryption techniques targeted at safeguarding IoT networks, providing insight into recent security trends within the IoT network sector. Our study's conclusions about the security dangers associated with the Internet of Things highlight how new threats and vulnerabilities in data- and protocol-based attacks are widening the attack surface. This demonstrates how traditional defenses against dynamic attacks—like botnet incursions, DDoS attacks, and malicious node infiltration—are becoming less effective in diverse IoT systems.

A review of current research models indicates that the majority of solutions to security issues—especially those involving communication channel security and energy conservation—rely on alternative encryption techniques. IoT network security has been improved by the integration of technologies such as blockchain, elliptical cryptography functions, artificial intelligence-driven fuzzy logic techniques, and machine learning. Adoption of such intricate solutions has, however, also resulted in an increase in system complexity and less openness on the intended security requirements. This study reflects the continued efforts of scientific researchers worldwide in the aforementioned fields by tracking the progress of current communication technologies, protocols, and internationally recognized standards. However, there's still a lot of space for research and development in this area.

7. REFERENCES

[1] *Jayaram Nori*[*1] [*1]Broadcom Inc, USA. DOI :- https://www.doi.org/10.56726/IRJMETS53503

[2] M. Alazab, "The impact of cyber security threats on business continuity and disaster recovery plans," IEEE Access, vol. 8, pp. 168887-168900, 2020, doi: 10.1109/ACCESS.2020.3023340.

[3] Cybersecurity Ventures, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025," 2020.

[Online]. Available: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/. [Accessed: 15-Apr-2024].

[4] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A deep learning approach for network intrusion detection system," in Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies (formerly BIONETICS), New York, NY, USA, May 2016, pp. 21-26, doi:

10.4108/eai.3-12-2015.2262516.

[5] D. S. Berman, A. L. Buczak, J. S. Chavis, and C. L. Corbett, "A survey of deep learning methods for cyber security," Information, vol. 10, no. 4, p. 122, Apr. 2019, doi: 10.3390/info10040122.

[6] Ponemon Institute, "The 2020 Cost of Insider Threats Global Report," 2020. [Online]. Available:

https://www.observeit.com/2020costofinsiderthreat/. [Accessed: 15-Apr-2024].

[7] MarketsandMarkets, "AI in Cybersecurity Market," 2020. [Online]. Available:

https://www.marketsandmarkets.com/Market-Reports/ai-in-cybersecurity-market-224437074.html. [Accessed: 15-Apr-2024].

[8] J. Saxe and K. Berlin, "eXpose: A character-level convolutional neural network with embeddings for detecting malicious URLs, file paths and registry keys," arXiv preprint arXiv:1702.08568, 2017.

[9] C. Yin, Y. Zhu, J. Fei, and X. He, "A deep learning approach for intrusion detection using recurrent neural networks," IEEE Access, vol. 5, pp. 21954-21961, 2017, doi: 10.1109/ACCESS.2017.2762418.

[10] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems:

techniques, datasets and challenges," Cybersecurity, vol. 2, no. 1, p. 20, Dec. 2019, doi: 10. 1186/s42400 -019-0038-7.

[11] Kaspersky Lab, "Machine Learning in Cybersecurity: Hype or Reality?," 2020. [Online]. Available:

https://www.kaspersky.com/blog/machine-learning-cybersecurity-hype-reality/19744/. [Accessed: 15-Apr-2024].

[12] H. J. Liao, C. H. R. Lin, Y. C. Lin, and K. Y. Tung, "Intrusion detection system: A comprehensive review," Journal of Network and Computer Applications, vol. 36, no. 1, pp. 16-24, Jan. 2013, doi: 10. 1016/j. jnca. 2012. 09.004.

[13] FICO, "Explainable AI in Banking," 2020. [Online]. Available: https://www.fico.com/en/latestthinking/white-paper/explainable-ai-banking. [Accessed: 15-Apr-2024].

[14] Microsoft, "Microsoft Security Intelligence Report," 2020. [Online]. Available: https://www.microsoft.com/en-us/security/business/security-intelligence-report. [Accessed: 15-Apr2024].

[15] I. J. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and harnessing adversarial examples," arXiv preprint arXiv:1412.6572, 2014.

[16] N. Carlini and D. Wagner, "Towards evaluating the robustness of neural networks," in 2017 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, May 2017, pp. 39-57, doi: 10. 1109/SP. 2017. 49.

[17] A. Kurakin, I. Goodfellow, and S. Bengio, "Adversarial examples in the physical world," arXiv preprint arXiv:1607.02533, 2016.

[18] I. Amit, J. Matherly, W. Hewlett, Z. Xu, Y. Meshi, and Y. Weinberger, "Machine learning in cyber-security - problems, challenges and data sets," arXiv preprint arXiv:1812.07858, 2018. [18] Cisco, "Cisco Annual Internet Report (2018–2023)," 2020. [Online]. Available:

https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internetreport/white-paper-c11-741490.html. [Accessed: 15-Apr-2024].

[19] D. S. Berman, A. L. Buczak, J. S. Chavis, and C. L. Corbett, "A survey of deep learning methods for cyber security," Information, vol. 10, no. 4, p. 122, Apr. 2019, doi: 10.3390/info10040122.

[20] IBM, "The Quant Crunch: How the Demand for Data Science Skills is Disrupting the Job Market," 2017. [Online]. Available: https://www.ibm.com/downloads/cas/3RL3VXGA. [Accessed: 15-Apr-2024].

[21] KPMG, "Artificial intelligence: Insights, potential and challenges," 2019. [Online]. Available: https://home.kpmg/xx/en/home/insights/2019/09/artificial-intelligence-insights-potentialchallenges.html. [Accessed: 15-Apr-2024].

[22] European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation)," Official Journal of the European Union, vol. 119, pp. 1-88, May 2016.

[23] S. Bhatt, A. Nayyar, and S. C. Sharma, "Interpretable machine learning for network intrusion detection:

A comprehensive survey," IEEE Access, vol. 9, pp. 62737-62764, 2021, doi: 10. 1109/ACCESS. 2021.3074190.

[24] J. H. Jeon, B. Jang, and K. S. Park, "Blockchain-based secure data sharing architecture for collaborative intrusion detection systems," IEEE Access, vol. 8, pp. 130766-130778, 2020, doi: 10. 1109/ACCESS. 2020.3009898.

[25] C. Yin, J. Xi, R. Sun, and J. Wang, "Location privacy protection based on differential privacy strategy for big data in industrial internet of things," IEEE Transactions on Industrial Informatics, vol. 14, no. 8, pp. 3628-3636, Aug. 2018, doi: 10.1109/TII.2017.2773646.

[26] S. J. Nawaz, S. Sharma, S. Wyne, M. Patwary, and M. Asaduzzaman, "Quantum machine learning for 6G communication networks: State-of-the-art and vision for the future," IEEE Access, vol. 7, pp. 4631746350, 2019, doi: 10.1109/ACCESS.2019.2909490.

[27] A. Fawaz, M. Zeki, and M. H. Alsharif, "Quantum-assisted deep learning for cybersecurity: Opportunities and challenges," IEEE Access, vol. 9, pp. 73044-73060, 2021, doi: 10.1109/ACCESS.2021.3079241.

[28] T. Kim, B. Kang, M. Rho, S. Sezer, and E. G. Im, "A multimodal deep learning method for android malware detection using various features," IEEE Transactions on Information Forensics and Security, vol. 14, no. 3, pp. 773-788, Mar. 2019, doi: 10.1109/TIFS.2018.2866319.