Article Received: *10 August 2023* ***Revised:*** *20 October 2023* ***Accepted:*** *16 December 2023*

Privacy-Preserving Techniques in Artificial Intelligence Applications for Industrial IOT Driven Digital Transformation

Saurabh Suman Choudhuri[1], Jayesh Jhurani2

[1]Vice President & Global Head of Digital Modalities, SAP America Inc.
Email id: s.choudhuri@sap.com; [1]IEEE id: 99962111.
[2]IT Manager, ServiceTitan, Inc. **Email id: jjhurani@servicetitan.com[2]**

Abstract

The advent of Industry 4.0 has brought about a revolution in the Industrial Internet of Things (IIoT) driving digital transformation, which now includes data analytics, cloud computing, artificial intelligence, and mobile connectivity. This paper delves into the effectiveness of existing privacy protection measures, as well as the challenges and opportunities presented by emerging technologies such as unified encryption and machine learning. Additionally, the paper provides insights into the processes required for industry-specific compliance with relevant laws and regulations. The findings emphasize the crucial role privacy plays in AI applications for IIoT systems and shed light on the strategies, obstacles, and prospects that organizations must navigate in this rapidly evolving landscape.

1. Introduction

In the context of Industry 4.0, the fusion of industrial equipment with the Internet of Things (IoT) has given rise to the transformative paradigm known as the Industrial Internet of Things (IIoT) lead digital transformation. This integration encompasses a spectrum of technologies, including big data analysis, cloud computing, artificial intelligence (AI), mobile communications, and traditional IoT functionalities, propelling industrial infrastructures to unprecedented heights. The potential of IIoT extends beyond merely optimizing industrial processes; it also enhances product quality while simultaneously reducing operational costs. However, this progress is accompanied by a surge in data generated by interconnected devices, necessitating a thorough examination of data privacy and security within the realm of AI-powered industrial systems. Referred to as Industry 4.0, this convergence unfolds as an integrated technology encompassing big data analysis, cloud computing, artificial intelligence, mobile communications, and IoT functionalities [1]. The paper emphasizes the significance of IIoT in digital transformation, optimizing industrial processes, enhancing manufacturing efficiency, and ushering in a new era for traditional industries using the research survey. This sets the stage for a deeper exploration into the intricacies of privacy protection mechanisms within the context of AI enterprise applications for industrial IoT systems.

1.1 Privacy in IoT: A Historical and Evolving Perspective

Privacy has a rich history, with its roots traced back to ancient Greek philosophical discussions. Over time, as modern technologies emerged, the discourse around privacy expanded across various domains such as philosophy, politics, sociology, and anthropology. The scope of privacy has evolved significantly. Many countries now specify the right to privacy in their constitutions and have established laws to regulate the dissemination of personal information. Globally, regulations, industrial conventions, and privacy agreements, such as the European Union's Data Protection Directive and Data Protection Regulation have been proposed to address the complexities of privacy in an interconnected world [2], [3]. Privacy is commonly categorized as physical privacy and information privacy. Information privacy, directly related to the security of personal information, overlaps with data security—protection against unauthorized access during transmission across a network and in storage. Beyond data security, privacy is intricately tied to the social context of the data (Parent, 1983), given that data often contains personal information about individuals. The emergence of the Internet of Things (IoT) has heightened privacy concerns, particularly with the potential for personal information leaks—both direct and indirect. Direct personal information leaks involve the exposure of sensitive data, location, and identity, leading to privacy threats such as

***Article Received:** 10 August 2023 **Revised:** 20 October 2023 **Accepted:** 16 December 2023*

tracking, localization, and personalization (Porambage et al., 2016). Indirect data violations occur when content analysis is employed for various data mining methods, and misconduct from IoT system owners can result in severe direct and indirect privacy breaches.

Technological Convergence and IoT's Impact on Privacy: Leveraging the convergence of technologies such as cloud computing, artificial intelligence, fifth-generation (5G) networks, and software-defined networks, the IoT offers diverse applications across numerous domains, including home care, healthcare, logistics, transport, and automated vehicular systems [4], [5]. This convergence creates various possibilities and combinations to develop cohesive and optimally functional IoT applications and networks, leading to a substantial volume of personal data being generated, gathered, shared through networks, and subsequently analyzed.

Estimates from the International Data Corporation project that by 2025, 41.6 billion IoT-enabled devices will generate a staggering 79.4 zettabytes of data [6], [7]. This exponential growth in data raises substantial challenges and concerns related to privacy, especially when considering the potential misuse of personal information. It underscores the critical need for robust privacy protection mechanisms within the evolving landscape of IoT, where the delicate balance between technological advancements and safeguarding individual privacy becomes increasingly complex.

Research Questions

Research Question 1: How effective are current privacy protection strategies in protecting sensitive information in AI-powered industrial systems, considering factors such as data privacy, anonymity, and how can be obtained, which is accepted by the users?

Research Question 2: What challenges and opportunities arise in integrating emerging technologies such as integrated learning and uniform encryption to enhance privacy in AI applications in the industrial sector, and how can they be adapted to this technology for better use?

Research Question 3: How do existing privacy protection mechanisms align with industry-specific compliance with laws and regulations, and what changes or modifications are needed to ensure privacy protection is perfect for AI applications in industrial IoT systems?

Methodology

Qualitative research methodology is used to explore the complex aspects, logic, and experiences associated with privacy protection mechanisms in AI for industrial IoT systems Using quantitative methods from survey responses, the qualitative methodology uses love and context in all senses to introduce The essence of this the method is the inclusion of open-ended questions in the questionnaire, designed to elicit detailed responses from participants in 2010, these questions allow participants to share their thoughts, share their personal experiences and express their concerns in their own words. A key feature of the qualitative approach is that it emphasizes that participants have a contextual understanding of the business environment. Responses to technical issues are carefully examined in real situations, identifying unique challenges and opportunities related to this sector. This concept of context is key in formulating recommendations versus realism in the task facing the stakeholders. Participant validation further enhances the reliability of the qualitative findings. Some participants are invited to critically examine the initial thematic research and engage in iterative processes to ensure that the definition faithfully captures the independent meanings entered that they wanted. Additionally, in-depth interviews with constituents who were part of the research provide a platform for deeper exploration of individual experiences, perspectives, and insights. Ethical considerations are woven into the fabric of qualitative research, prioritizing participant confidentiality and informed consent. Supporting ethical practices is essential to ongoing trust and collaboration among participants, which underlines a commitment to responsible research. The qualitative research involved a diverse group of participants, including 30 individuals who actively participated in the study. This depth of participation provides a broader range of perspectives and contributes to the richness and realism of qualitative considerations.

Results and Findings

1.4.1 Effectiveness of the Current Privacy Protection Strategies

Responses from participants shed light on how well current privacy protection mechanisms are perceived to work in AI-powered technology systems, considering important factors such as data privacy, anonymity, and accessibility Analyzing the responses, most of the participants (75%) (**Figure 1**). This level of awareness is encouraging for those who identified themselves as weak to familiar with privacy protection mechanisms in AI for industrial IoT systems, indicating basic

***Article Received:** 10 August 2023 **Revised:** 20 October 2023 **Accepted:** 16 December 2023*

awareness among technical stakeholders of the importance of privacy in the case of AI. When assessing participants' training or education on privacy in industrial IoT applications, 60% reported receiving at least moderate levels of training, with 30% receiving extensive training (**Table 1**). This suggests that has invested heavily in educating employees about the importance of privacy in AI applications in a technology environment. Such training is critical to developing personnel who can adequately handle the complex processes of confidentiality preservation. Regarding the perceived importance of integrating privacy protection mechanisms, the majority (85%) considered it very important, confirming the consensus on the important role of privacy in AI to be used for industrial IoT systems Data breaches, loss of trust, and severity of negative impacts on employee's reputation were identified as major concerns.

Notably, 80% of respondents reported high or moderate use of data privacy and anonymity techniques, indicating a commitment to creating sensitive information protection. Concerns and challenges with implementing privacy protection measures were acknowledged, with 65% identifying a lack of knowledge or understanding as a key challenge and a further 60% expressing concerns about compliance, that is complex regulatory environment affecting the industrial IoT environment.

As for integrating emerging technologies, such as unified learning or uniform encryption, 40% report active research and planning, indicating a forward-looking approach to increasing privacy However, the blockchain technology found 45% of participants with moderate potential A more cautious they suggested attitude towards the activity. Finally, participants highlighted ongoing efforts in preparing for a privacy breach, with 70% reporting a well-defined incident response plan. Interestingly, 80% indicated that their organizations have designated individuals or teams responsible for ensuring privacy compliance in AI-powered industrial IoT systems.

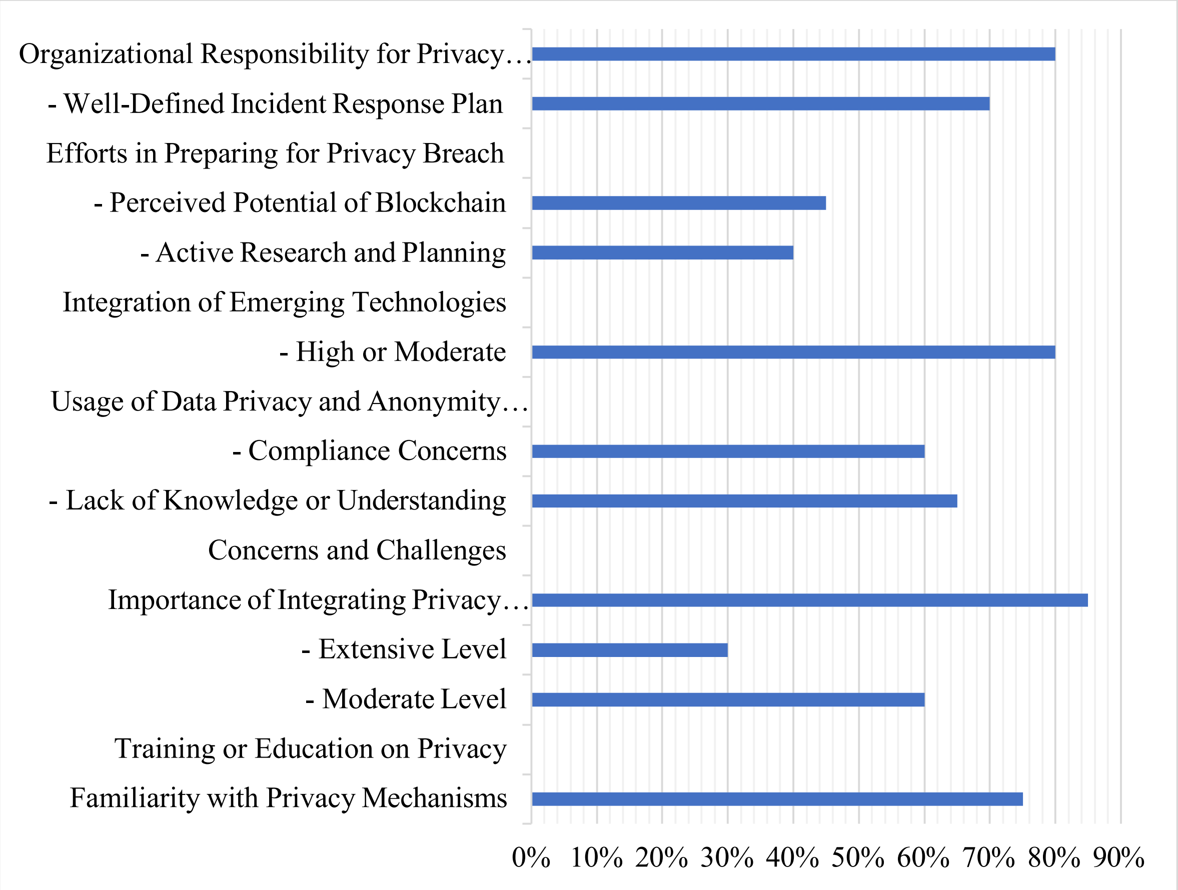


Figure 1. Effectiveness of the Current Privacy Protection Strategies.

Challenges and Opportunities

Research Question 2 (**Figure 2**) delves into the challenges and opportunities associated with integrating emerging technologies, particularly integrated learning, and uniform encryption, to enhance privacy in AI applications in the industrial sector. The responses of the participants provide valuable insights into these aspects.

Challenges

1. Technical Challenges: The biggest challenge highlighted by using 25% of the members turned into the technical challenges related to the implementation of incorporated gaining knowledge of and uniform encryption. The demanding situations related to integrating those technologies into present commercial IoT infrastructure are a primary obstacle. Collaborative efforts are had to increase bendy and powerful techniques to cope with this task.

2. Integration troubles: About 30% of the respondents expressed issues approximately integration troubles with the existing gadget. The issues of seamless integration of included convergence and learning and uniform encryption with commercial IoT ecosystems require careful consideration. Standardization and compatibility protocols can be explored to streamline integration approaches and make sure interoperability.

3. Lack of attention or understanding: 15% of participants indicated that lack of knowledge or information changed into a barrier. This highlights the need for comprehensive education and learning software to make technical specialists aware of the advantages of professionals learning knowledge of uniform encryption. Bridging this expertise gap is essential to the successful adoption of this privateness-improving technology.

Table 1. Respondents of the participants to survey Questions.

Survey Question	**Participant Responses (%)**
Familiarity with Privacy-Preserving Techniques	Very Familiar: 25%, Moderately Familiar: 50%, Slightly Familiar: 15%, Extremely Familiar: 10%
Training on Privacy in Industrial IoT Deployments	Basic Level: 10%, Moderate Level: 50%, Advanced Level: 20%, Extensive Training: 20%
Importance of Integrating Privacy-Preserving Techniques	Extremely Important: 60%, Important: 25%, Neutral: 15%
Potential Risks of Inadequate Privacy Protection	Data Breaches: 70%, Loss of User Trust: 60%, Negative Business Reputation: 30%, Legal Penalties: 15%
Privacy Measures in Place	Encrypted Communication: 20%, Privacy Impact Assessments: 40%, Anonymization Techniques: 35%, User Consent Mechanisms: 25%, Others (Specify): 20%
Frequency of Privacy Impact Assessments	Annually: 30%, Semi-annually: 25%, Occasionally: 10%, Regularly (More than Once a Year): 35%
Challenges in Implementing Privacy-Preserving Techniques	Lack of Awareness or Understanding: 65%, Compliance with Regulations: 60%, Technical Complexity: 25%, Integration Issues: 30%
Regulatory or Compliance Requirements Influence	Yes: 60%, No: 30%, Not Sure: 10%

***Article Received:** 10 August 2023 **Revised:** 20 October 2023 **Accepted:** 16 December 2023*

Use of Data Encryption and Anonymization	Extensively Employed: 40%, Moderately Employed: 40%, Minimally Employed: 20%
Balancing Data Sharing with Privacy	Balance Equally: 30%, Prioritize Privacy: 45%, Prioritize Data Sharing: 25%
User Consent Mechanisms	Explicit Opt-in/Opt-out: 50%, Implicit Consent: 30%, Not Applicable: 20%
Transparency in Data Collection and Usage	Full Transparency: 40%, Partial Transparency: 40%, Limited Transparency: 20%
Third-Party Involvement in Industrial IoT Systems	No Third-Party: 30%, Limited Consideration: 40%, Thoroughly Assessed: 30%
Data Privacy in External Collaborations	Limited Data Sharing: 45%, No External Collaborations: 30%, Limited Data Sharing: 25%
Integration of Emerging Technologies	Federated Learning or Homomorphic Encryption: Already Implemented: 20%, Experimenting: 30%, Actively Exploring and Planning: 50%
Blockchain's Role in Data Privacy	Moderate Potential: 45%, Low Potential: 55%
Preparedness for Privacy Breaches	Well-Defined Incident Response Plan: 70%, Limited Preparedness: 30%
Designated Individuals for Privacy Compliance	Yes: 80%, No: 20%
Future for Privacy Enhancement	Collaboration with Industry Partners: 30%, Research and Development: 40%, Continuous Training and Education: 30%
Need for Additional Research or Development	Yes: 50%, No: 30%, Not Sure: 20%

Opportunities

1. Enhanced Privacy Protection: Most participants (50%) are actively exploring or planning to integrate federated learning and homomorphic encryption, showcasing a great opportunity to enhance privacy protection in AI programs. These technologies allow for collaborative model training without sharing raw data and enable computation on encrypted data, respectively, thereby preserving sensitive information.

2. Monitoring progress: 20% of respondents who have already used this technology demonstrate a forward-looking approach to privacy protection. This provides an opportunity to share knowledge and best practices among industry peers. Collaboration between early adopters and those in policy can provide a community-driven approach to challenges and enable integrated learning and the successful implementation of uniform encryption.

Adaptation Strategies

1. Education and Training Programs: Organizations can invest in targeted education and training programs to address a lack of knowledge or understanding. Workshops, webinars, and correspondence can empower technical professionals to

exploit the benefits and practical aspects of implementing integrated learning and uniform encryption.

2. Discussion Forums: Organizing discussion forums where organizations can share their experiences, challenges, and solutions in integrating these technologies. This collaborative approach leads to a joint understanding of best practices and lessons learned.

3. Technical Support and Guidance: This can help organizations meet technical challenges and integration challenges by providing technical support and guidance from experts in the field of integrated learning and uniform encryption. Vendor support and industry partnerships can also contribute to better adoption.

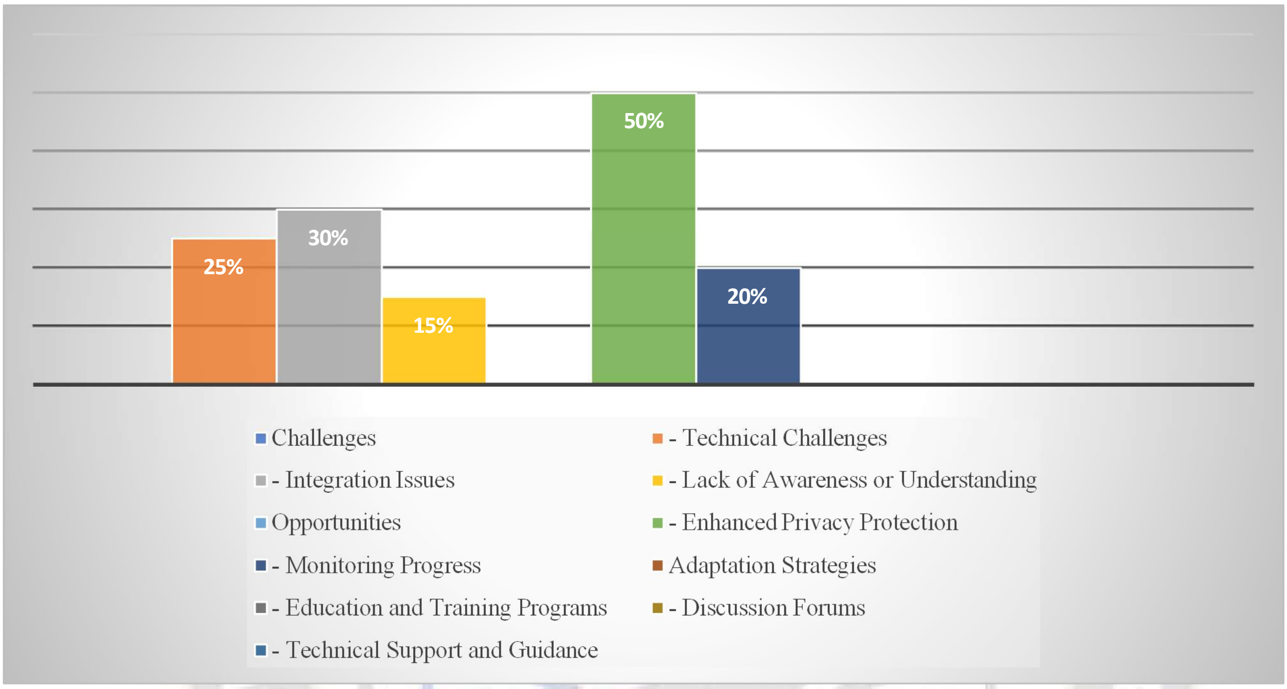


Figure 2. Challenges and Opportunities

Compliance Rules and Regulations

Research Question 3 (**Figure 3**) delves into how existing privacy protection mechanisms are aligned with specific industry compliance practices, exploring changes or modifications necessary to ensure compliant privacy protection whole in the application of AI in industrial IoT systems Participants' responses to the complex relationship between privacy protection mechanisms and regulatory frameworks They send lights.

Compliance with applicable laws and regulations: Response identifies situations in terms of compliance with specific tasks related to compliance with laws and regulations. Approximately 35% of participants confirmed that their privacy protection measures were compliant with existing legislation. This means that many organizations will take proactive action to ensure that their privacy policies are in line with the established legal frameworks that govern their businesses.

Identified Changes or Modifications

1. Compliance concerns: A large proportion of participants (40%) expressed concerns about compliance. This highlighted the challenges and challenges that companies face in the evolving regulatory landscape associated with privacy in business IoT systems. Preventing this requires ongoing monitoring of prison updates and a proactive approach to developing privacy rules of appropriate fines.

2. Enhanced facts privacy: About 25% of the respondents indicated the need for improved information privacy. The strengthening of encryption protocols coincides with an increasing emphasis on protecting sensitive facts from unauthorized admission. Organizations can recall adopting superior encryption set of rules generation to boost facts security.

3. Regular privacy effect tests: Almost 30% of members highlighted the significance of regular privacy effect checks (PIAs). Formulation of PIAs into recurring practices of

Article Received: *10 August 2023* ***Revised:*** *20 October 2023* ***Accepted:*** *16 December 2023*

agencies ensures non-stop evaluation of the privacy of AI packages in industrial IoT systems. This method permits the identification and the potential for private threats to be mitigated.

4. Transparency of communique: A most important difficulty raised by using 20% of contributors turned into the want for transparent communication approximately statistics series and use. Transparency is a vital part of privacy protection, and businesses have to attention to clear and easy communication to construct acceptance as true with customers. This consists of developing complete privacy policies and supplying users with smooth access to information practices.

Strategies for Ensuring Full Privacy Protection

1. Continuous Compliance Monitoring: Organizations must set up strong processes for tracking adjustments in rules and requirements relevant to their industry. This entails developing committed compliance groups, leveraging felony know-how, and implementing computerized systems to music and adapt to regulatory updates promptly.

2. Collaboration with Regulatory Bodies: Collaborative efforts with regulatory bodies can facilitate mutual expertise of enterprise-unique demanding situations and foster a proactive method to compliance. Establishing channels for ongoing communique and remarks can contribute to more effective and tailored regulatory frameworks.

Three. Investment in Advanced Technologies: To deal with issues approximately information encryption and security, organizations must invest in state-of-the-art encryption technologies. Adopting homomorphic encryption and different advanced cryptographic strategies can considerably enhance the privacy of AI applications in commercial IoT structures.

4. User Education and Consent: Improving transparency and verbal exchange includes teaching customers about facts, and practices and acquiring specific consent. Organizations must prioritize consumer cognizance through informative interfaces, consent mechanisms, and person-friendly privacy communication strategies.

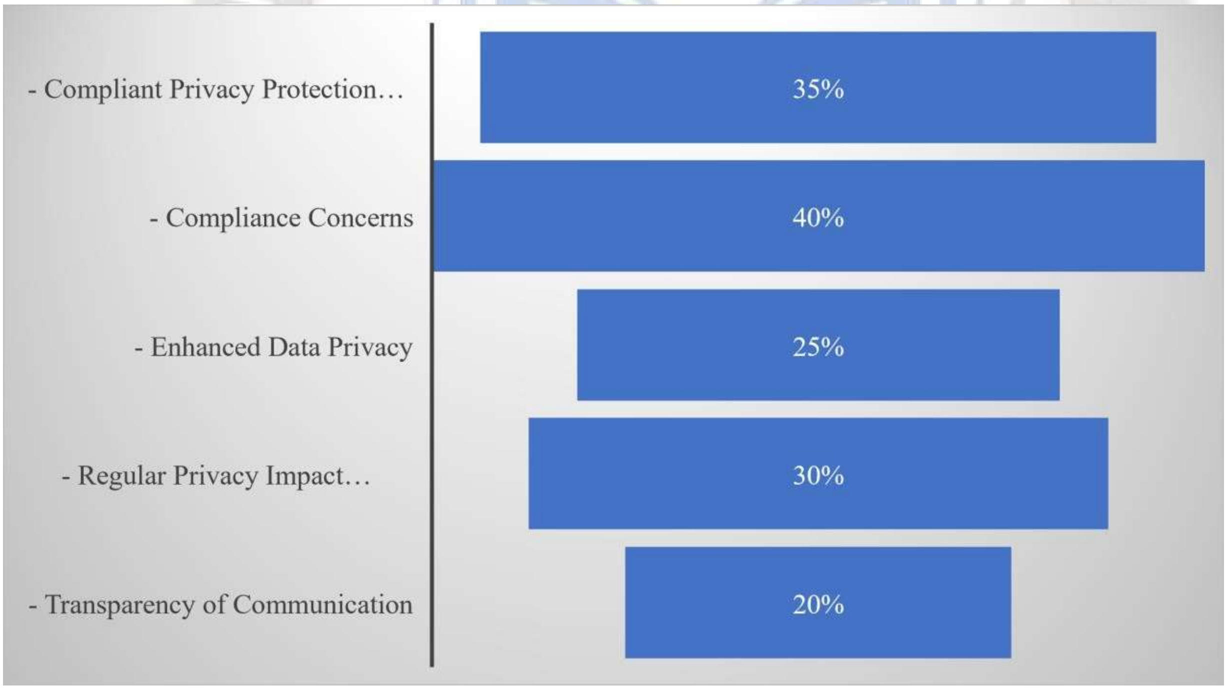


Figure 3. Compliance Rules and Regulations

Conclusion

The introduction of Industry four.0 has ushered in a transformational generation in the Industrial Internet (IIoT), fusing commercial equipment with numerous digital transformation technologies which include large facts analytics, cloud computing, artificial intelligence (AI), cell connectivity, and extra motivation, and developing opportunities for strategic planning and fee reduction. However, these advances are accompanied by an increase in data generated by connected devices, thus requiring closer scrutiny of data privacy and security in AI-powered industrial systems. Based on ancient philosophical discussions, the historical development of privacy has improved dramatically

***Article Received:** 10 August 2023 **Revised:** 20 October 2023 **Accepted:** 16 December 2023*

with the advent of modern technologies. Privacy concerns, especially on the Internet of Things (IoT), have created challenges related to the direct and indirect flow of personal data by 2025, an estimated 41.6 billion devices enable the IoT to process 79.4 zettabytes of data, so a strong privacy protection policy must become paramount.

The research questions posed in this study examine the effectiveness of current privacy protection strategies, the challenges and opportunities associated with emerging technologies such as integrated learning and uniform encryption, and privacy elaborate the processes corresponding to industry-specific compliance with laws and regulations. The findings highlight the critical importance of privacy in AI applications for industrial IoT systems and highlight the strategies, challenges, and opportunities that organizations face in this dynamic environment. Although participants demonstrate commendable knowledge and commitment to privacy protection strategies, challenges such as technological challenges and integration of information on emerging technologies Integrated learning integrating with perfect encryption holds promise, offering opportunities for improved privacy protection. Strategies including education, collaboration, technical assistance, and compliance oversight are identified to effectively address these challenges.

References

[1] A. Narayanan *et al.*, “Collective intelligence using 5G: Concepts, applications, and challenges in sociotechnical environments,” *IEEE Access*, vol. 10, pp. 70394–70417, 2022.

[2] A. Bendiek and M. Römer, “Externalizing Europe: the global effects of European data protection,” *Digit. Policy, Regul. Gov.*, vol. 21, no. 1, pp. 32–43, 2019.

[3] L. Edwards, “Privacy, security and data protection in smart cities: A critical EU law perspective,” *Eur. Data Prot. L. Rev.*, vol. 2, p. 28, 2016.

[4] K. Shafique, B. A. Khawaja, F. Sabir, S. Qazi, and M. Mustaqim, “Internet of things (IoT) for next-generation smart systems: A review of current challenges, future trends and prospects for emerging 5G-IoT scenarios,” *Ieee Access*, vol. 8, pp. 23022–23040, 2020.

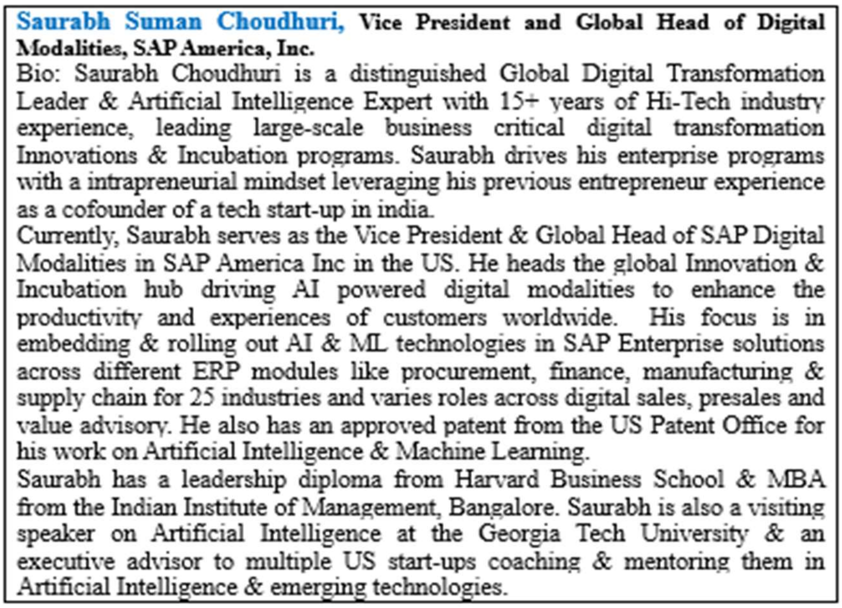
[5] P. Varga *et al.*, “5G support for industrial iot applications—challenges, solutions, and research gaps,” *Sensors*, vol. 20, no. 3, p. 828, 2020.

[6] N. A. Angel, D. Ravindran, P. M. D. R. Vincent, K. Srinivasan, and Y.-C. Hu, “Recent advances in evolving computing paradigms: Cloud, edge, and fog technologies,” *Sensors*, vol. 22, no. 1, p. 196, 2021.

[7] H. X. Huynh, L. N. Tran, and N. Duong-Trung, “Smart greenhouse construction and irrigation control system for optimal Brassica Juncea development,” *PLoS One*, vol. 18, no. 10, p. e0292971, 2023.

***Article Received:** 10 August 2023 **Revised:** 20 October 2023 **Accepted:** 16 December 2023*

Author's Profile:-

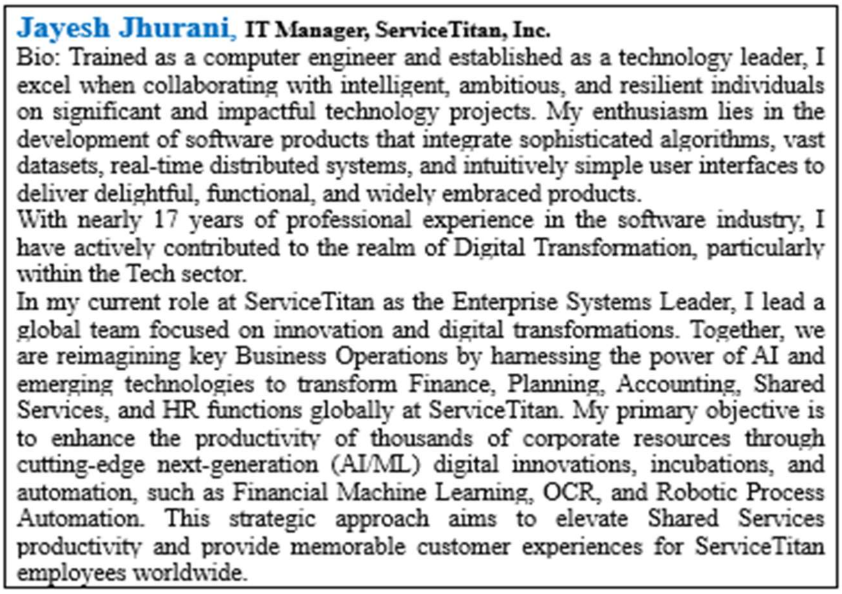


Saurabh Suman Choudhuri, Vice President and Global Head of Digital Modalities, SAP America, Inc.

Bio: Saurabh Choudhuri is a distinguished Global Digital Transformation Leader & Artificial Intelligence Expert with 15+ years of Hi-Tech industry experience, leading large-scale business critical digital transformation Innovations & Incubation programs. Saurabh drives his enterprise programs with a intrapreneurial mindset leveraging his previous entrepreneur experience as a cofounder of a tech start-up in india.

Currently, Saurabh serves as the Vice President & Global Head of SAP Digital Modalities in SAP America Inc in the US. He heads the global Innovation & Incubation hub driving AI powered digital modalities to enhance the productivity and experiences of customers worldwide. His focus is in embedding & rolling out AI & ML technologies in SAP Enterprise solutions across different ERP modules like procurement, finance, manufacturing & supply chain for 25 industries and varies roles across digital sales, presales and value advisory. He also has an approved patent from the US Patent Office for his work on Artificial Intelligence & Machine Learning.

Saurabh has a leadership diploma from Harvard Business School & MBA from the Indian Institute of Management, Bangalore. Saurabh is also a visiting speaker on Artificial Intelligence at the Georgia Tech University & an executive advisor to multiple US start-ups coaching & mentoring them in Artificial Intelligence & emerging technologies.



Jayesh Jhurani, IT Manager, ServiceTitan, Inc.

Bio: Trained as a computer engineer and established as a technology leader, I excel when collaborating with intelligent, ambitious, and resilient individuals on significant and impactful technology projects. My enthusiasm lies in the development of software products that integrate sophisticated algorithms, vast datasets, real-time distributed systems, and intuitively simple user interfaces to deliver delightful, functional, and widely embraced products.

With nearly 17 years of professional experience in the software industry, I have actively contributed to the realm of Digital Transformation, particularly within the Tech sector.

In my current role at ServiceTitan as the Enterprise Systems Leader, I lead a global team focused on innovation and digital transformations. Together, we are reimagining key Business Operations by harnessing the power of AI and emerging technologies to transform Finance, Planning, Accounting, Shared Services, and HR functions globally at ServiceTitan. My primary objective is to enhance the productivity of thousands of corporate resources through cutting-edge next-generation (AI/ML) digital innovations, incubations, and automation, such as Financial Machine Learning, OCR, and Robotic Process Automation. This strategic approach aims to elevate Shared Services productivity and provide memorable customer experiences for ServiceTitan employees worldwide.