The Impact Of Data Breaches On Consumer Trust In E-Commerce

[1]Dr.Mamta Kumari, Assistant Professor, Department Of Management , L.N.Mishra Institute of Economic Development and Social Change Patna,Bihar, India

[2]Pallav Chandra Sinha, Assistant Professor, BSc.IT, College Of Commerce Arts and Science, Magadh University, Gaya, Bihar, India

[3]Sannu Priya, Student, BCA, Catalyst Evening College, Patna, Bihar, India

Abstract: Data breaches have been a wide and concerning issue in the digital world, affecting e-commerce businesses and their customers. The paper is a review of the complex relationship between data breaches and consumer trust within the domain of e-commerce. Businesses may face prominent consequences in case of a data breach, which means unauthorized access to sensitive consumer information and may include financial losses, reputational damage, and erosion of consumer trust. The paper considers a synthesis of the literature on how data breaches affect consumers' trust, based on studies and case examples that cover a wide range. The paper reviews the underlying theory of consumer trust in e-commerce, assumed to be part and parcel of customer relationship building for successful business operations. Secondly, it proceeds to look at various kinds of data breaches and their immediate and long-term consequences on consumer trust. Finally, key findings are drawn from notable case studies for the Target and Equifax data breaches that demonstrate the range of impacts on consumer behavior and trust recovery efforts. The review also focuses on strategies businesses use to recover lost trust after suffering data breaches. These strategies are assessed for their effectiveness in mollifying the concerns of consumers and restoring confidence in them to prevent future breaches. This identifies common themes and gaps in literature that can add valuable insight into what factors influence the successful recovery of lost trust. The paper concludes with major insights taken from the literature, underlining that the study in reality requires further research to continue to strengthen the dynamic changes between data breaches and consumer trust. Second, it creates practical implications for e-commerce businesses by providing them with recommendations on improving cybersecurity practices and enhancing consumer trust. The overall contribution of this review to the literature on how data breaches affect consumer trust delivers actionable insights that would help businesses navigate and mitigate the impacts of a data breach within the e-commerce environment..

Keywords: Data Breaches, Consumer Trust, E-Commerce, Cybersecurity, Trust Recovery, Consumer Behavior, Trust Repair, Case Studies.

1. Introduction

Data breaches have become a significant issue in the digital age, posing severe risks to businesses and consumers alike. In the e-commerce sector, where transactions often involve sensitive personal and financial information, data breaches can lead to catastrophic outcomes. These breaches result in unauthorized access to confidential data, which can be exploited for fraudulent activities, identity theft, and other malicious purposes. The immediate aftermath of a data breach often includes financial losses, legal ramifications, and substantial reputational damage for the affected company [1]. However, one of the most profound and lasting impacts of data breaches is the erosion of consumer trust. Trust is a foundational element of e-commerce, influencing consumer behavior, purchase decisions, and brand loyalty. When consumers perceive that their data is not secure, they are likely to reduce their online activities, switch to competitors, or avoid e-commerce platforms altogether. Understanding the dynamics of how data breaches affect consumer trust is crucial for developing effective strategies to mitigate these adverse effects and restore confidence in online transactions.

1.1.Objectives of the Review

This review paper aims to explore and synthesize existing research on the impact of data breaches on consumer trust within the e-commerce sector. The primary objectives of this review are [2]:

1. To analyze how data breaches influence consumer trust in e-commerce platforms.
2. To examine the immediate and long-term consequences of data breaches on consumer behavior.
3. To identify factors that exacerbate or mitigate trust erosion following data breaches.
4. To evaluate the effectiveness of various trust recovery strategies employed by e-commerce businesses.
5. To provide actionable insights and recommendations for e-commerce businesses to enhance cybersecurity measures and rebuild consumer trust post-breach.

By addressing these objectives, this review seeks to provide a comprehensive understanding of the complex relationship between data breaches and consumer trust, offering valuable insights for both academic researchers and industry practitioners.

1.2 Scope of the Review

The scope of this review encompasses a broad range of data breaches in the e-commerce sector, focusing on incidents that have occurred over the past decade. The review includes various types of data breaches, such as those resulting from hacking, phishing, malware, and insider threats. It covers a diverse array of e-commerce platforms, including major online retailers, financial service providers, and digital marketplaces. The review synthesizes findings from empirical studies, theoretical research, industry reports, and notable case studies to provide a well-rounded perspective on the issue. By defining these boundaries, the review ensures a focused and relevant analysis, offering insights that are applicable to a wide range of e-commerce contexts [3].

2. Theoretical background

2.1 Consumer Trust in E-Commerce

Consumer trust in e-commerce refers to the confidence consumers have in the safety, reliability, and integrity of online transactions and the entities facilitating these transactions. Trust is a crucial element in e-commerce as it influences consumers' willingness to engage in online shopping, share personal information, and make purchases. High levels of trust lead to increased consumer loyalty, repeat purchases, positive word-of-mouth, and overall customer satisfaction [4]. Without trust, consumers are hesitant to provide their personal and financial information, which can significantly hinder the growth and success of e-commerce businesses. Several theoretical frameworks have been developed to understand consumer trust in e-commerce. The Trust Building Model suggests that consumer trust is built through a combination of factors such as website design, privacy policies, security features, and past experiences. Positive interactions and the perceived professionalism of an e-commerce site enhance trust. The Technology Acceptance Model (TAM) posits that perceived ease of use and perceived usefulness are primary determinants of consumer acceptance of technology, including e-commerce platforms. Trust is influenced by how easy and beneficial consumers perceive the online shopping experience to be. The Institution-Based Trust framework emphasizes the role of institutional mechanisms, such as regulatory compliance, third-party certifications, and reputation, in building consumer trust. Consumers are more likely to trust e-commerce platforms that adhere to recognized standards and regulations. Lastly, the Risk-Trust Model focuses on the relationship between perceived risk and trust, suggesting that higher perceived risk in online transactions can decrease trust. Conversely, effective risk mitigation strategies can enhance trust. Understanding these frameworks helps in analyzing how trust is formed, maintained, and eroded in the context of e-commerce [5].

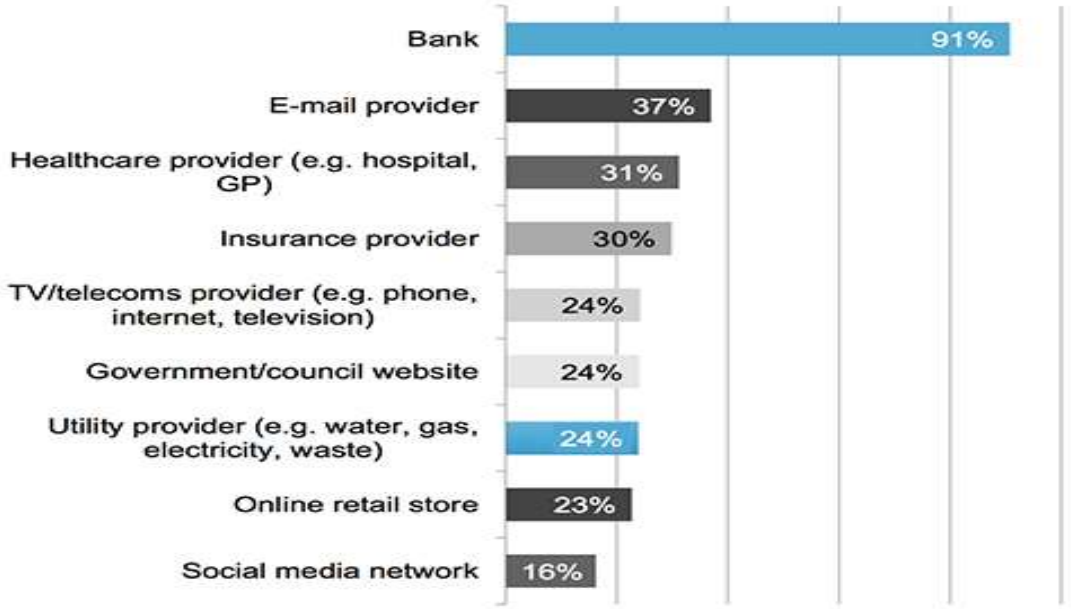

Fig 1. Type of Consumer Concerns [Source : helpnetsecurity.com]

2.2 Data Breaches

A data breach is an incident in which sensitive, confidential, or protected information is accessed, disclosed, or used by an unauthorized individual. Data breaches can occur due to various reasons, including cyberattacks, insider threats, or system vulnerabilities. In the e-commerce sector, the most common types of data breaches include hacking, phishing, malware, insider threats, and human error. Hacking involves unauthorized access to e-commerce systems through techniques such as phishing, malware, ransomware, and SQL injection. Phishing refers to fraudulent attempts to obtain sensitive information by disguising as a trustworthy entity in electronic communications. Malware is malicious software designed to disrupt, damage, or gain unauthorized access to computer systems. Insider threats are breaches caused by employees or other insiders who have legitimate access to the system but misuse their privileges. Human error involves the accidental exposure of sensitive information due to negligence or lack of proper security protocols [6]. The implications of data breaches are far-reaching and multifaceted, affecting both businesses and consumers. Financial losses are a significant consequence for businesses, which may incur costs related to breach detection, response, legal fees, and compensation for affected consumers. Consumers may suffer financial losses due to fraud and identity theft. Reputational damage is another critical consequence, as the loss of consumer trust and negative publicity can severely damage a company's reputation, leading to decreased customer loyalty and revenue. Legal and regulatory consequences also arise, as companies may face fines and sanctions for failing to protect consumer data adequately. They are required to comply with data protection regulations like GDPR and CCPA. For consumers, the impact of data breaches includes stress, inconvenience, and financial hardship. They may become more hesitant to engage in online transactions, affecting their overall online shopping experience. Additionally, data breaches can disrupt business operations, leading to downtime, loss of productivity, and increased costs for implementing new security measures. By defining and understanding the types and implications of data breaches, businesses can better prepare and respond to such incidents, ultimately working towards maintaining consumer trust [7].

3. Impact of Data Breaches on Consumer Trust

3.1 Immediate Effects

Research consistently shows that data breaches have an immediate and profound impact on consumer trust. When a data breach occurs, consumers often react with a significant loss of confidence in the affected e-commerce platform [8]. This loss of confidence is driven by the fear that their personal and financial information has been compromised, potentially leading to fraudulent activities and identity theft. Consumers

may immediately change their behavior in response to a breach, such as reducing or halting their online shopping activities with the affected retailer. A survey by PwC found that 87% of consumers stated they would take their business elsewhere if they felt their data was not being handled responsibly, highlighting the swift and decisive actions consumers are willing to take when their trust is compromised. Furthermore, consumers often expect immediate and transparent communication from the company regarding the breach, and any delay or perceived lack of transparency can exacerbate the loss of trust. Studies indicate that the way a company handles the immediate aftermath of a breach—through timely notifications, clear explanations, and offers of support—plays a crucial role in either mitigating or intensifying the initial erosion of trust [8].

3.2 Long-Term Consequences

The long-term consequences of data breaches on consumer trust are equally significant and can lead to lasting damage to a company's reputation and customer relationships. Longitudinal studies suggest that the impact of a data breach extends far beyond the immediate aftermath, with lasting effects on consumer trust and loyalty. Consumers who experience a breach may develop a heightened sense of skepticism and caution when engaging with the affected e-commerce platform, often resulting in a sustained decline in transaction volumes and customer retention rates. For instance, a study by the Ponemon Institute found that businesses affected by data breaches experienced an average customer turnover rate increase of 5%, which could result in substantial revenue losses over time. Additionally, the breach may lead to a broader reputational damage that affects not only existing customers but also potential new customers who may be deterred by the negative publicity surrounding the breach. Long-term trust erosion can also manifest in a shift in consumer attitudes towards data security and privacy, with customers becoming more selective and demanding higher security assurances from e-commerce platforms. As trust is a foundational element of customer loyalty, its erosion can have a cascading effect, diminishing brand equity and competitive advantage in the market [9].

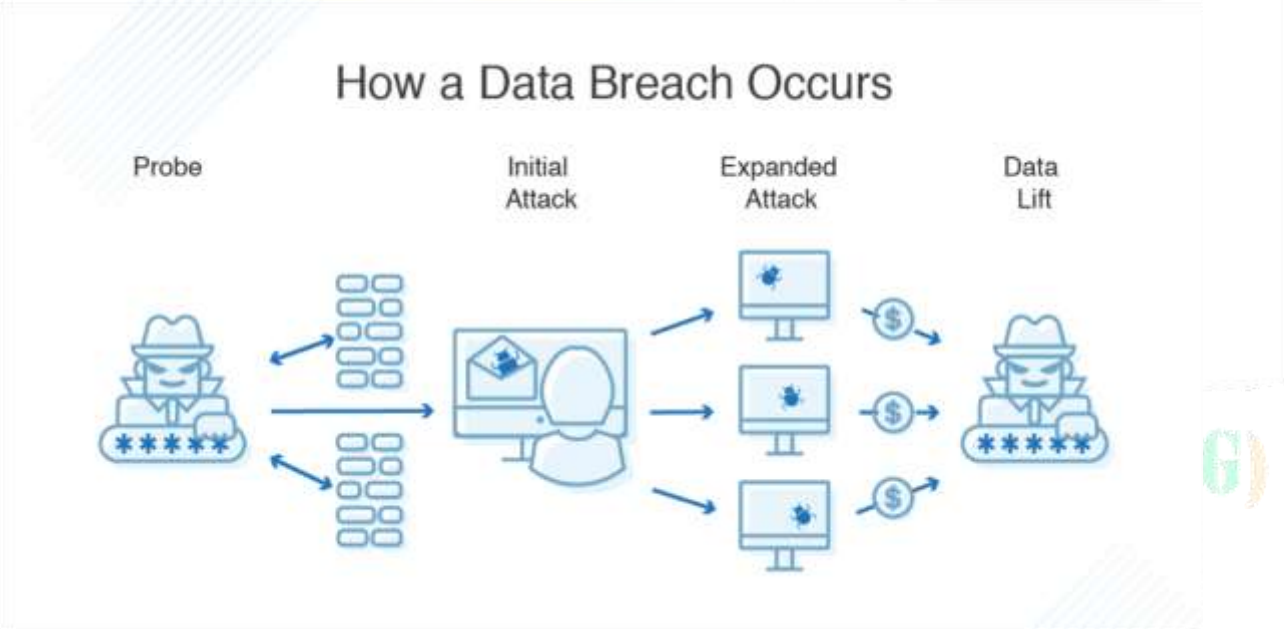

Fig 2. Data Breaches [Source: Dnsstuff.com]

3.3 Factors Influencing Trust Erosion

Several factors influence the extent to which a data breach erodes consumer trust. One critical factor is the severity of the breach, which includes the volume and sensitivity of the data compromised. Breaches involving highly sensitive information, such as financial details or personal identifiers, tend to result in more significant trust erosion compared to breaches involving less sensitive data. The company's response to the breach is another crucial factor. Effective and timely communication, taking responsibility, and providing clear guidance on protective measures can help mitigate the negative impact on trust. Conversely, poor communication, attempts to downplay the breach, or delays in notifying affected consumers can exacerbate trust erosion. Media coverage also plays a pivotal role in shaping public perception and trust. Extensive media coverage highlighting the breach, particularly if it focuses on the company's perceived failings in data protection, can amplify the loss of trust. Studies have shown that proactive and transparent communication strategies, along with visible efforts to enhance security measures post-breach, can help rebuild trust over time. Additionally, third-party endorsements or certifications that verify the implementation of robust security

protocols can assist in restoring consumer confidence. Understanding these factors is essential for e-commerce businesses aiming to navigate the complex landscape of trust recovery following a data breach [10].

4. Case Studies and Examples

Case Study 1: Target Data Breach (2013)

Summary of the Breach and Its Impact: In December 2013, Target Corporation experienced one of the largest data breaches in retail history. The breach occurred during the peak holiday shopping season, compromising the credit and debit card information of approximately 40 million customers and the personal information, including names, addresses, phone numbers, and email addresses, of an additional 70 million individuals. The breach was orchestrated by cybercriminals who gained access to Target's network through a third-party vendor's credentials, eventually infiltrating the point-of-sale (POS) system to install malware that captured payment card data.

How It Affected Consumer Trust and the Company's Recovery Efforts: The immediate impact on consumer trust was profound. Customers were alarmed by the scale of the breach and the potential misuse of their financial information. Many consumers lost confidence in Target's ability to protect their data, leading to a noticeable decline in store visits and online transactions. Target's initial response, which included delayed notifications and a perceived lack of transparency, further exacerbated the erosion of trust. In the months following the breach, Target undertook significant recovery efforts, including offering free credit monitoring services to affected customers, enhancing security measures, and appointing a new Chief Information Security Officer (CISO). Despite these efforts, the company struggled to regain consumer trust quickly, facing legal battles and incurring substantial financial costs estimated at over $200 million. Over time, Target's commitment to improved cybersecurity and transparent communication helped in partially restoring consumer confidence, though the brand's reputation was indelibly marked by the breach [11].

Case Study 2: Equifax Data Breach (2017)

Summary of the Breach and Its Impact: In September 2017, Equifax, one of the largest credit reporting agencies in the world, disclosed a massive data breach that exposed the personal information of approximately 147 million consumers. The compromised data included names, Social Security numbers, birth dates, addresses, and, in some cases, driver's license numbers and credit card information. The breach was particularly alarming due to the sensitive nature of the data and the scale of the exposure. Cybercriminals exploited a vulnerability in a web application framework that Equifax had failed to patch, allowing them to gain unauthorized access to the company's systems.

Long-Term Effects on Consumer Trust and the Company's Response: The long-term effects on consumer trust were severe and far-reaching. Given Equifax's role as a custodian of sensitive financial data, the breach shattered consumer confidence not only in Equifax but also in the broader credit reporting industry. Many consumers were outraged by the company's delayed disclosure of the breach, which occurred several months after the initial discovery, and the lack of immediate protective measures offered. Equifax's response involved offering free credit monitoring and identity theft protection services, along with a comprehensive website for consumers to check if they were affected. Despite these efforts, the company faced intense scrutiny from regulators and lawmakers, resulting in fines and settlements totalling over $700 million. The breach had a lasting impact on Equifax's reputation, with trust in the company's data security measures remaining significantly impaired. Consumers continued to express heightened concerns about the safety of their personal information, leading to increased demand for regulatory reforms and improved data protection standards across the industry [12].

Case Study 3: Recent Data Breach Examples

Provide Examples of More Recent Data Breaches and Their Impact on Consumer Trust: More recent examples of data breaches continue to highlight the ongoing challenges businesses face in protecting consumer information and maintaining trust. For instance, the 2019 Capital One data breach exposed the personal information of over 100 million customers, including credit scores, credit limits, balances, payment history, and contact information. The breach was attributed to a misconfigured firewall, which allowed an unauthorized individual to access the data stored in Amazon Web Services (AWS). The immediate aftermath saw a sharp decline in consumer trust, with many customers questioning the security of their financial information.

Another notable example is the 2020 Marriott International data breach, which exposed the personal information of approximately 5.2 million guests. The breach was a result of unauthorized access to login credentials of two Marriott employees. This incident followed a previous breach in 2018 that compromised the data of 500 million guests, compounding the trust issues consumers had with the hotel chain. The recurrence of breaches within a short period severely damaged Marriott's reputation and consumer trust, with many customers opting to stay with competitors perceived as more secure.

These recent breaches underscore the critical importance of robust cybersecurity measures and the need for companies to be vigilant in protecting consumer data. The repeated occurrence of breaches also highlights the growing consumer awareness and sensitivity to data security issues, making trust recovery even more challenging for affected companies. The impact on consumer trust in these cases demonstrates the necessity for businesses to prioritize transparency, timely communication, and proactive security enhancements to mitigate the adverse effects of data breaches on their reputation and customer relationships.

6. Related Works

Okeke, R. I., et al. 2013, Despite the rapid growth in e-commerce, most of these lines of privacy and trust issues are still far from solution. A qualitative study that looked into customer concerns about privacy and issues of trust in online shopping, covering data privacy, security, and sharing with third parties, revealed that users are more comfortable if the website is trusted, secure, and has clear protection policies; unsecured websites stating their policies vaguely do not encourage the sharing of personal data [13].

Brilliant, M. A., & Achyar, A. (2013): Despite increasing trends of using the internet and e-commerce, Indonesia is far behind in research into e-commerce compared to other Asian nations. This study has been conducted in order to find out the influence of customer satisfaction and trust towards loyalty in e-commerce. The results found an impact of information quality on trust and trust on loyalty. For customer loyalty in e-commerce, websites should provide credible information regarding the product's quality [14].

Mubarak Alharbi et al. (2013): This paper aims to extend knowledge of the approach as perceived by customers for privacy and security by studying the issues of privacy concerns and data security, together with the elements of these concerns. In this explanatory design, the researcher samples data from six organizations and four customer focus groups. The result in this research work was key areas of CPPS and the realization of the need for PbD in organizational practices. The findings are helpful in developing a general conceptual model geared toward better understanding CPPS and its impact on the success of e-commerce [15].

Matbouli, H., & Gao, Q. (2012, March): While e-commerce has hugely evolved to offer convenience, speed, and safety in consumerism, security-related issues make many consumers still leery of spending online. The paper surveys e-commerce security concerns impacting its success with strategies to mitigate risks. It also evaluates the barriers to e-commerce adoption in developing nations, proposing solutions to cross them [16].

Velmurugan, M. S., 2012, The growth of the Internet and e-commerce has so many issues related to security, privacy, and trust. This study tried to find the same in Malaysia, especially on their implications for the protection of consumers in e-commerce transactions. Out of the ten variables investigated, six were significant, which had to do with authentication and personal integrity, and four were non-significant, relating

to encryption and consumer trust. Some recommendations are made on how to enhance consumer protection in Malaysian e-commerce [17].

Table 1. Literature Review Findings

Author Name (Year)	Main Concept	Findings
Okeke, R. I., et al. (2013)	Privacy and trust issues in e-commerce	Trusted, secure websites with clear data protection policies increase user comfort and reduce data privacy concerns, while unsecured sites with vague policies discourage data sharing.
Brilliant, M. A., & Achyar, A. (2013)	Customer satisfaction and trust in e-commerce	Information quality influences trust, which in turn affects customer loyalty. E-commerce websites should focus on providing reliable product information to build trust and loyalty.
Mubarak Alharbi, I., et al. (2013)	Customers' perceived privacy and security (CPPS)	Identified key areas of CPPS and emphasized Privacy by Design (PbD) in organizational practices. Findings help develop a conceptual model to understand CPPS and its impact on e-commerce success.
Matbouli, H., & Gao, Q. (2012, March)	E-commerce security issues and solutions	Surveys and analyzes e-commerce security issues, offering strategies to mitigate risks. Examines barriers to e-commerce adoption in developing countries and suggests solutions.
Velmurugan, M. S. (2012)	Security, privacy, and trust issues in Malaysian e-commerce	Six variables, including authentication and personal integrity, significantly impact consumer protection in e-commerce transactions. Recommendations are made for improving consumer protection in Malaysia.

These studies all point to lingering privacy, trust, and security problems that have an overall bearing on customer behavior and the eventual success of online transactions. For example, Okeke et al. established in 2013 that the secure website with clearly stated data protection policies allayed feelings regarding the privacy of customers, and those websites not secure would not encourage customers to divulge their data. Brilliant and Achyar proved in 2013 that high-quality information had a positive effect on customer loyalty and trust in Indonesian e-commerce. Alharbi et al. (2013) focused on how PbD could address the CPPS of the customer and hence contributed to developing a conceptual model for the understanding of these issues in a better way. Matbouli and Gao (2012) provided measures for minimizing and dealing with security risks in e-commerce and identified barriers to its adoption in developing nations. Velmurugan (2012) identified key factors that affected consumer protection in the Malaysian e-commerce atmosphere, also providing recommendations to enhance security and trust. All of these studies underline the fact that strong privacy, security, and trust measures are needed to develop consumer confidence and loyalty in the use of e-commerce.

8. Challenges

Sentiment Analysis Challenges

- **Nuance in Consumer Sentiment:** Accurately capturing the complex emotional responses (Sinha R., (2013)) of consumers to data breaches, which may include anger, fear, betrayal, and uncertainty, presents a significant challenge[18].
- **Data Bias:** The available sentiment data may be skewed towards highly emotional reactions, potentially overlooking subtle changes in consumer trust over time.
- **Contextual Understanding:** Comprehending the context of consumer sentiment, such as the type of data breached or the company's response, is crucial but difficult to capture accurately.

Decision Tree Algorithm Challenges

- **Feature Engineering:** Identifying and selecting the most relevant features that impact consumer trust, such as breach severity, industry type, company reputation, and consumer demographics, is a complex task.
- **Handling Complex Interactions:** Sinha R.,(2014) Decision trees may struggle to capture the intricate relationships between various factors influencing consumer trust[19].
- **Dynamic Trust Landscape:** Consumer trust is influenced by multiple, evolving factors, making it challenging to build a static decision tree model that accurately predicts trust levels over time.

7. Conclusion

Surgical robots powered by AI are quantum leaps in medical technology. Human surgeons teaming up with AI-driven robotic systems provides precision, accuracy, and efficacy to surgical procedures. One such synergy brings together strengths—human expertise and intuitive judgment—with the computational power and consistency of AI that enhances decision-making, reduces variability, and improves outcomes for patients. Historical and technical advances in both robotics and AI set the stage for these innovations, while continued technical advancements continue to push the boundaries of what can be done in surgical care. Importantly, AI algorithms—especially machine learning models, computer vision, and reinforcement learning—have contributed much to the precision and adaptability of surgical robots. It is through advances in hardware robotics and sophisticated integration techniques that perfect collaboration between human surgeons and AI systems can be realized with optimized surgical workflow and enhanced decision support in real time. Furthermore, AI's role in surgical training and simulation puts surgeons in a position where they can be well-prepared in using these technologies effectively, culminating in continuous improvements in surgical proficiency and patient safety. From this, AI-enhanced surgical robots will bring a number of advantages to the health sector, including precision and accuracy in surgery, strong decision-supportive systems for surgeons, and increased efficiency in surgical operations, which would directly or indirectly bring about better patient outcomes and decreased cost of treatment. With innovation in AI only progressing at high speed, the potential of AI to transform surgical practices also becomes very obvious. On the ethical and regulatory challenges thrown out by AI integrations, addressing those has to be very careful to avoid any kind of patient harm or leakage of their data. A future for surgical robotics will totally depend on improvements in AI technology, further interdisciplinary collaboration, and sustained human-AI teams in continued acts to drive innovation. Only then, through sustained use of this collaborative edge for human-AI teams, will the medical profession reach unprecedented levels of surgical excellence and quality care available for patients globally. This paper emphasizes embracing such innovations and a forward-thinking approach to surgical practice aimed at betterment in the quality of life and health outcome for all.

References

1. Reddy, A. (2012). A study on consumer perceptions on Security, Privacy and Trust on E-Commerce Portals. *International Journal of Multidisciplinary Management Studies*, *2*(3), 1-15.
2. Beatty, P., Reay, I., Dick, S., & Miller, J. (2011). Consumer trust in e-commerce web sites: A meta-study. *ACM Computing Surveys (CSUR)*, *43*(3), 1-46.
3. Najafi, I. (2012). The role of e-commerce awareness on increasing electronic trust. *Life Science Journal*, *9*(4), 1487-1494.
4. Smith, K. T. (2011). CONSUMER PERCEPTIONS REGARDING E-COMMERCE AND RELATED RISKS. *B> Quest*.
5. Niranjanamurthy, M., & Chahar, D. (2013). The study of e-commerce security issues and solutions. *International Journal of Advanced Research in Computer and Communication Engineering*, *2*(7), 2885-2895.

6. Maniam, B., Naranjo, L., & Subramaniam, G. (2012). E-commerce best practices: How to achieve an environment of trust and security. *International Journal of Innovation, Management and Technology*, *3*(4), 396.
7. Hussain, M. A. (2013). A study of information security in e-commerce applications. *International Journal of Computer Engineering Science (IJCES)*, *3*(3), 1-9.
8. Ayyagari, R. (2012). An exploratory analysis of data breaches from 2005-2011: Trends and insights. *Journal of Information Privacy and Security*, *8*(2), 33-56.
9. Boritz, J. E., & No, W. G. (2011). E-commerce and privacy: Exploring what we know and opportunities for future discovery. *Journal of Information Systems*, *25*(2), 11-45.
10. McCrohan, K., & Harvey, J. W. (2011, April). SECURITY IN INTERNET COMMERCE: EMERGING THREATS TO CUSTOMER TRUST. In *American Institute of Higher Education 6 th International Conference Proceedings Volume 4–Number* (p. 262).
11. Garbarino, E., & Maxwell, S. (2010). Consumer response to norm-breaking pricing events in e-commerce. *Journal of Business Research*, *63*(9-10), 1066-1072.
12. Dwyer, C. A. (2011). The effect of behavioral targeting on trust in e-commerce. *Available at SSRN 1801366*.
13. Okeke, R. I., Shah, M. H., & Ahmed, R. (2013). Issues of privacy and trust in e-commerce: Exploring customers' perspective. *Journal of Basic and Applied Scientific Research*, *3*(3), 571-577.
14. Brilliant, M. A., & Achyar, A. (2013). The impact of satisfaction and trust on loyalty of e-commerce customers. *ASEAN Marketing Journal*, *5*(1), 4.
15. Mubarak Alharbi, I., Zyngier, S., & Hodkinson, C. (2013). Privacy by design and customers' perceived privacy and security concerns in the success of e-commerce. *Journal of Enterprise Information Management*, *26*(6), 702-718.
16. Matbouli, H., & Gao, Q. (2012, March). An overview on web security threats and impact to e-commerce success. In *2012 International Conference on Information Technology and e-Services* (pp. 1-6). IEEE.
17. Velmurugan, M. S. (2012). An empirical analysis of consumers' protection toward e-commerce transactions in Malaysia. *International journal of business Information systems*, *9*(3), 295-327.
18. Sinha R, Jain R., "Mining Opinions from Text: Leveraging Support Vector Machines for Effective Sentiment Analysis ISSN: 2321-1776 , Impact Factor: 3.5, Vol.01 Issue-05, (Sep, 2013), Page: 15-25
19. Sinha R, Jain R., "Decision Tree Applications for Cotton Disease Detection: A Review of Methods and Performance Metrics" International Journal in Commerce, IT & Social Sciences; ISSN: 2394-5702 , Vol.1 Issue-02, (November 2014),Page: 63-73