ई-कॉमर्स में सुरक्षा और एन्क्रिप्शन की अवधारणा और आवश्यकता

Security And *Encryption* Concept And Need In *Ecommerce*

ई-कॉमर्स में, सुरक्षा ऑनलाइन स्टोर और ग्राहक डेटा को साइबर खतरों से बचाने के उपायों का एक ढाँचा है, जबकि एन्क्रिप्शन एक मुख्य अवधारणा है जो संवेदनशील डेटा को एक अपठनीय कोड में परिवर्तित करके ट्रांसमिशन और स्टोरेज के दौरान अनधिकृत पहुँच को रोकती है। धोखाधड़ी को रोकने, वित्तीय और व्यक्तिगत जानकारी की सुरक्षा करने, कानूनी अनुपालन सुनिश्चित करने और ऑनलाइन खरीदारों का विश्वास बनाए रखने के लिए, अंततः व्यवसाय को वित्तीय नुकसान और प्रतिष्ठा को नुकसान से बचाने के लिए दोनों की आवश्यकता सर्वोपरि है।

ई-कॉमर्स सुरक्षा की अवधारणा

Concept of E-Commerce Security

ई-कॉमर्स सुरक्षा में लेन-देन और डेटा प्रबंधन के लिए एक सुरक्षित ऑनलाइन वातावरण बनाने हेतु उपयोग किए जाने वाले उपकरण और अभ्यास शामिल हैं। इसमें शामिल हैं:

- **डेटा एन्क्रिप्शन:**

क्रेडिट कार्ड नंबर और पासवर्ड जैसी संवेदनशील जानकारी को एक कोड में बदलना जिसे केवल अधिकृत पक्ष ही डिक्रिप्ट कर सकते हैं।

- **SSL/TLS (सिक्योर सर्वर लेयर/ट्रांसपोर्ट लेयर सिक्योरिटी)**

प्रमाणपत्र:

ये प्रमाणपत्र HTTPS प्रोटोकॉल को सक्षम करते हैं, जो किसी वेबसाइट और उसके आगंतुकों के बीच आदान-प्रदान किए गए डेटा को एन्क्रिप्ट करता है, जिससे एक सुरक्षित कनेक्शन बनता है (ब्राउज़र में एक पैडलॉक आइकन द्वारा दर्शाया जाता है)।

• सुरक्षित भुगतान गेटवे:

पेपैल और स्ट्राइप जैसे प्लेटफ़ॉर्म जो लेनदेन को सुरक्षित रूप से संभालते हैं, अक्सर एन्क्रिप्शन का उपयोग करते हैं और PCI-DSS जैसे मानकों का अनुपालन करते हैं।

• मल्टी-फैक्टर ऑथेंटिकेशन (MFA):

उपयोगकर्ताओं को अपने खातों तक पहुँचने के लिए एक से अधिक प्रकार के सत्यापन प्रदान करने की आवश्यकता होती है।

• साइबर सुरक्षा उपाय:

विभिन्न साइबर हमलों से बचाव के लिए फ़ायरवॉल, एंटी-मैलवेयर सॉफ़्टवेयर और अन्य सुरक्षात्मक उपकरणों का कार्यान्वयन।

ई-कॉमर्स में सुरक्षा और एन्क्रिप्शन की आवश्यकता

Need for Security and Encryption in E-commerce

• ग्राहक डेटा की सुरक्षा:
क्रेडिट कार्ड विवरण, पते और व्यक्तिगत जानकारी जैसी संवेदनशील जानकारी को चोरी और धोखाधड़ी से सुरक्षित रखना।

• **वित्तीय नुकसान की रोकथाम:**
डेटा उल्लंघनों और अनधिकृत लेनदेन से होने वाले वित्तीय नुकसान से व्यवसाय और उसके ग्राहकों, दोनों की सुरक्षा करना।

• **कानूनी अनुपालन सुनिश्चित करना:**
डेटा सुरक्षा और गोपनीयता के लिए नियामक आवश्यकताओं, जैसे PCI-DSS, को पूरा करना।

• **ग्राहक विश्वास का निर्माण:**
ग्राहकों द्वारा लेनदेन पूरा करने और सुरक्षा के प्रति प्रतिबद्धता प्रदर्शित करने वाले व्यवसायों के प्रति वफ़ादार बने रहने की संभावना अधिक होती है।

• **व्यावसायिक प्रतिष्ठा बनाए रखना:**
डेटा उल्लंघन से प्रतिष्ठा को भारी नुकसान हो सकता है, जिससे विश्वास में कमी और व्यवसाय में गिरावट आ सकती है।

• **डेटा अखंडता सुनिश्चित करना:**
एन्क्रिप्शन यह सुनिश्चित करने में मदद करता है कि डेटा को ट्रांज़िट के दौरान दुर्भावनापूर्ण तत्वों द्वारा इंटरसेप्ट या परिवर्तित न किया जाए।

ई-कॉमर्स सुरक्षा:

E-commerce Security:

• ई-कॉमर्स सुरक्षा मूल रूप से ई-कॉमर्स प्लेटफ़ॉर्म के लिए विशेष रूप से डिज़ाइन किए गए प्रोटोकॉल के एक सेट से संबंधित है ताकि इलेक्ट्रॉनिक लेनदेन को सुरक्षित रूप से संसाधित किया जा सके। ई-

कॉमर्स सुरक्षा इंटरनेट पर पूर्ण सुरक्षा और संरक्षा के साथ सामान खरीदने और बेचने में मदद करती है।

• ई-कॉमर्स सुरक्षा के अभाव में ग्राहकों के बैंकिंग क्रेडेंशियल्स का नुकसान, उपयोगकर्ताओं की निजी संवेदनशील जानकारी का लीक होना, फ़िशिंग हमले, धन की चोरी और क्रेडिट कार्ड से संबंधित धोखाधड़ी होती है।

• इलेक्ट्रॉनिक भुगतान प्रणाली, जो ई-कॉमर्स सुरक्षा का एक अनिवार्य हिस्सा है, उपयोगकर्ता के अनुकूल तरीके से संचालन में मदद करती है और कठिन दस्तावेज़ीकरण प्रक्रियाओं से बचाती है और लेनदेन की कुछ लागत भी बचाती है।

• ई-कॉमर्स सुरक्षा इलेक्ट्रॉनिक भुगतान प्रणालियों को सुरक्षा प्रदान करने में सक्षम बनाती है ताकि वे आसानी से डेटा संसाधित कर सकें और सुरक्षित तरीके से इलेक्ट्रॉनिक धन हस्तांतरित कर सकें।

ई-कॉमर्स सुरक्षा वातावरण (आयाम)

E Commerce Security Environment(Diamension)

ई-कॉमर्स सुरक्षा परिवेश के आयाम गोपनीयता, अखंडता, उपलब्धता, प्रामाणिकता, अस्वीकृती और निजता हैं। ये मूलभूत सिद्धांत सुनिश्चित करते हैं कि संवेदनशील जानकारी अनधिकृत पहुँच से सुरक्षित रहे, डेटा सटीक और अपरिवर्तित रहे, सिस्टम और डेटा ज़रूरत पड़ने पर सुलभ हों, उपयोगकर्ताओं और डेटा स्रोतों की पहचान सत्यापित हो, लेन-देन को गलत तरीके से नकारा न जा सके, और व्यक्तिगत डेटा व्यक्ति द्वारा नियंत्रित हो।

• **गोपनीयता:**
यह सुनिश्चित करता है कि केवल अधिकृत व्यक्ति ही संवेदनशील जानकारी तक पहुँच सकें, और इसे अनधिकृत प्रकटीकरण से सुरक्षित रखता है।

• **अखंडता:**
यह गारंटी देता है कि डेटा और जानकारी अपने पूरे जीवनचक्र में सटीक, पूर्ण और अपरिवर्तित रहें, जिससे अनधिकृत संशोधनों को रोका जा सके।

• **उपलब्धता:**
यह सुनिश्चित करता है कि ई-कॉमर्स प्रणाली और उसका डेटा अधिकृत उपयोगकर्ताओं के लिए जब भी और जहाँ भी आवश्यकता हो, सुलभ और उपलब्ध हो।

• **प्रामाणिकता:**
उपयोगकर्ताओं की पहचान और डेटा के स्रोत की पुष्टि करता है, यह सुनिश्चित करता है कि जानकारी दावा किए गए स्रोत से आती है और उपयोगकर्ता वही हैं जो वे होने का दावा करते हैं।

• **अस्वीकृति न करना:**
लेनदेन में शामिल पक्षों को घटना के बाद अपनी भागीदारी या कार्यों से इनकार करने से रोकता है।

• **गोपनीयता**:
उपयोगकर्ताओं को उनके व्यक्तिगत डेटा पर नियंत्रण प्रदान करता है, यह निर्धारित करता है कि उनकी जानकारी कैसे एकत्रित, उपयोग और साझा की जाती है।

ई-कॉमर्स सुरक्षा का दायरा

Scope Of E-Commerce Security

ई-कॉमर्स सुरक्षा का दायरा ग्राहक डेटा की सुरक्षा करना, विश्वास बनाए रखना, सेवाओं की निर्बाध उपलब्धता सुनिश्चित करना, वित्तीय नुकसान को रोकना और एसएसएल/टीएलएस एन्क्रिप्शन, मल्टी-फैक्टर ऑथेंटिकेशन (एमएफए), मजबूत भुगतान गेटवे और पीसीआई डीएसएस और जीडीपीआर जैसे मानकों के पालन जैसे उपायों के माध्यम से नियामक अनुपालन की गारंटी देना है।

- **डेटा सुरक्षा:**

ई-कॉमर्स सुरक्षा में व्यक्तिगत जानकारी और भुगतान विवरण सहित संवेदनशील ग्राहक डेटा को अनधिकृत पहुँच और उल्लंघनों से सुरक्षित रखना शामिल है।

- **ग्राहक विश्वास:**

ग्राहक विश्वास का निर्माण और उसे बनाए रखना अत्यंत महत्वपूर्ण है, क्योंकि सुरक्षा संबंधी चूक ई-कॉमर्स प्लेटफ़ॉर्म में विश्वास को कम कर सकती है, जिससे उसकी प्रतिष्ठा और राजस्व पर असर पड़ सकता है।

- **वित्तीय सुरक्षा:**

धोखाधड़ी वाले लेनदेन, डेटा उल्लंघनों और धन के अनधिकृत उपयोग से होने वाले वित्तीय नुकसान को रोकने के लिए उपाय किए जाते हैं।

• **लेन-देन की अखंडता:**
यह सुनिश्चित करना कि लेन-देन सही ढंग से और सहमति के अनुसार संसाधित हों, ताकि ऑर्डर खो न जाएँ या गलत जगह न पहुँचें।

• **उपलब्धता:**
यह सुनिश्चित करना कि ई-कॉमर्स प्लेटफ़ॉर्म ग्राहकों और व्यावसायिक भागीदारों के लिए लगातार उपलब्ध और सुलभ रहे।

• **गोपनीयता:**
यह सुनिश्चित करना कि ई-कॉमर्स लेनदेन के दौरान प्रेषित जानकारी निजी रहे और अनधिकृत व्यक्तियों के लिए दुर्गम रहे।

• **प्रमाणीकरण और प्राधिकरण:**
उपयोगकर्ता की पहचान सत्यापित करना और यह सुनिश्चित करना कि उनके पास विशिष्ट जानकारी तक पहुँचने या लेनदेन करने के लिए सही अनुमतियाँ हैं।

• **अस्वीकृति न करना:**
किसी ऑनलाइन लेनदेन में अपनी भागीदारी से इनकार करने से पक्षों को रोकने के लिए एक तंत्र प्रदान करना।

ई-कॉमर्स के लिए खतरों के प्रकार:

Types of threats to E-commerce:

• **कर चोरी:** संगठन आईआरएस को राजस्व के कानूनी कागजी रिकॉर्ड दिखाते हैं। लेकिन ई-कॉमर्स खरीदारी के मामले में, ऑनलाइन लेनदेन होते हैं, जिसके कारण धनराशि इलेक्ट्रॉनिक रूप से स्थानांतरित हो जाती है, जिससे आईआरएस लेनदेन की सही गणना नहीं कर पाता और इन संगठनों द्वारा कर चोरी की संभावना अधिक होती है।

• **भुगतान विवाद:** ई-कॉमर्स में, उपयोगकर्ताओं और ई-कॉमर्स प्लेटफ़ॉर्म के बीच भुगतान विवाद उत्पन्न हो सकते हैं। ये इलेक्ट्रॉनिक धन हस्तांतरण प्रणालियाँ उपयोगकर्ताओं से अतिरिक्त लेनदेन संसाधित कर सकती हैं, जिससे कुछ गड़बड़ियों या त्रुटियों के कारण उपयोगकर्ताओं द्वारा भुगतान विवाद उत्पन्न हो सकता है।

• **वित्तीय धोखाधड़ी:** जब भी कोई ऑनलाइन लेनदेन या धन हस्तांतरण होता है, तो यह हमेशा प्रमाणीकरण के लिए कुछ पिन या पासवर्ड मांगता है और केवल अधिकृत व्यक्ति को ही लेनदेन संसाधित करने की अनुमति देता है। लेकिन हमलावरों द्वारा उपयोग किए जाने वाले कुछ स्पाइवेयर और वायरस के कारण, वे अनधिकृत व्यक्ति को अनुमति देकर उपयोगकर्ताओं के लेनदेन को भी संसाधित कर सकते हैं, जिससे उपयोगकर्ता के साथ वित्तीय धोखाधड़ी हो सकती है।

• **ई-वॉलेट:** ई-वॉलेट अब ई-कॉमर्स प्लेटफ़ॉर्म का एक अनिवार्य हिस्सा हैं। ई-वॉलेट पर हमले से उपयोगकर्ताओं की संवेदनशील बैंकिंग

जानकारी लीक हो सकती है जिसका इस्तेमाल हमलावर अपने फायदे के लिए कर सकते हैं। नियामक उपयोगकर्ताओं के धन की वित्तीय सुरक्षा से जुड़ी सभी गतिविधियों पर नज़र रखते हैं।

• **फ़िशिंग:** यह आजकल उपयोगकर्ताओं पर होने वाले सबसे आम हमलों में से एक है, जिसमें हमलावर बड़ी संख्या में उपयोगकर्ताओं को ईमेल और संदेश भेजते हैं जिनमें एक विशेष लिंक होता है। जब उपयोगकर्ता उस लिंक को अपने ब्राउज़र में खोलते हैं, तो मैलवेयर बैकग्राउंड में डाउनलोड होना शुरू हो जाता है और हमलावर उपयोगकर्ता की वित्तीय जानकारी पर पूरा नियंत्रण हासिल कर लेता है।
उपयोगकर्ताओं को अपनी वेबसाइट पर विश्वास दिलाने और उनके वित्तीय क्रेडेंशियल भरने के लिए वे नकली वेबसाइट बनाते हैं।

• **SQL इंजेक्शन**: SQL इंजेक्शन का इस्तेमाल हमलावर बड़े संगठनों के डेटाबेस में हेरफेर करने के लिए करते हैं। हमलावर डेटाबेस में मैलवेयर से भरा दुर्भावनापूर्ण कोड डालते हैं और फिर डेटाबेस में लक्षित क्वेरीज़ खोजते हैं और फिर डेटाबेस की सभी संवेदनशील जानकारी एकत्र कर लेते हैं।

• **क्रॉस-साइट स्क्रिप्टिंग (XSS):** हैकर ई-कॉमर्स कंपनियों की वेबसाइट के कोडबेस में दुर्भावनापूर्ण कोड डालकर उन्हें निशाना बनाते हैं। यह एक बहुत ही हानिकारक हमला है क्योंकि पूरी वेबसाइट का नियंत्रण हमलावरों के हाथों में चला जाता है। यह हमलावरों को उपयोगकर्ताओं की ब्राउज़िंग गतिविधि और उनकी कुकीज़ का उपयोग करके उन्हें ट्रैक करने में सक्षम बना सकता है। अधिक

जानकारी के लिए कृपया क्रॉस-साइट स्क्रिप्टिंग XSS क्या है लेख पढ़ें।

• **ट्रोजन:** हमलावर ऐसे सॉफ़्टवेयर बनाते हैं जो डाउनलोड करने से पहले उपयोगी लग सकते हैं, लेकिन सॉफ़्टवेयर डाउनलोड होने के बाद यह कंप्यूटर पर सभी दुर्भावनापूर्ण प्रोग्राम इंस्टॉल कर देता है। यह व्यक्तिगत विवरण, पता, ईमेल, वित्तीय क्रेडेंशियल जैसे डेटा एकत्र करता है और इससे डेटा लीक हो सकता है।

• **ब्रूट फ़ोर्स हमले**: हैकर किसी अनधिकृत उपयोगकर्ता के खाते में सेंध लगाने के लिए पैटर्न बनाते हैं और बेतरतीब तरीके अपनाते हैं। इसमें हमलावर द्वारा खाते का पासवर्ड तोड़ने के लिए कई एल्गोरिदम, क्रमपरिवर्तन और संयोजनों का उपयोग करना पड़ता है।

• **बॉट्स**: हैकर ई-कॉमर्स वेबसाइटों पर बड़ी संख्या में बॉट्स का इस्तेमाल करते हैं ताकि ई-कॉमर्स उद्योग में प्रतिस्पर्धियों की रैंकिंग और उनके उपयोगकर्ताओं की खरीदारी नीतियों पर नज़र रखी जा सके ताकि प्रतिस्पर्धी की बिक्री और राजस्व को कम किया जा सके। इससे उपयोगकर्ताओं को होने वाले खराब अनुभवों के कारण प्रतिस्पर्धियों की तुलना में उनकी ई-कॉमर्स वेबसाइट की रैंकिंग भी कम हो जाती है। इसके परिणामस्वरूप कुल कीमत में कमी आती है और बिक्री में कुल राजस्व कम होता है।

• **डीडीओएस हमले**: वितरित सेवा अस्वीकार (डीडीओएस) हमले आमतौर पर हैकर्स द्वारा मूल वैध उपयोगकर्ताओं को ई-कॉमर्स प्लेटफॉर्म पर उत्पादों तक पहुँचने और खरीदने-बेचने से रोकने के लिए किए जाते हैं। हैकर्स बड़ी संख्या में कंप्यूटरों का इस्तेमाल

करके सर्वर पर अनुरोधों की संख्या इतनी बढ़ा देते हैं कि एक समय सर्वर क्रैश हो जाता है।

• **स्किमिंग**: स्किमिंग, वेबसाइट के मुख्य पृष्ठों पर मैलवेयर फैलाने का एक लोकप्रिय तरीका है, जिसका इस्तेमाल बड़ी संख्या में लोग करते हैं। यह उस वेबपेज पर उपयोगकर्ताओं द्वारा दर्ज की गई सभी जानकारी चुरा लेता है और लीक कर देता है और यह सारी जानकारी स्किमिंग के ज़रिए हमलावर तक पहुँच जाती है।

• **बिचौलिए हमला**: इस प्रकार के हमले में, हमलावर उपभोक्ता और ई-कॉमर्स प्लेटफ़ॉर्म के बीच हो रही बातचीत की सारी जानकारी साफ़ तौर पर प्राप्त कर सकता है। हमलावर दोनों के बीच हो रही बातचीत को देखता है और इसे उपयोगकर्ता को किसी खतरे में डालने के अवसर के रूप में इस्तेमाल करता है।

सुरक्षा उल्लंघनों का प्रभाव

Impact of Security Breaches

• **डेटा चोरी:** व्यक्तिगत जानकारी, वित्तीय डेटा और लॉगिन क्रेडेंशियल्स का उल्लंघन।
• **वित्तीय हानि:** धोखाधड़ी से प्रत्यक्ष वित्तीय हानि और संभावित जुर्माना।
• **प्रतिष्ठा को नुकसान:** ग्राहक विश्वास की हानि और ब्रांड छवि को नुकसान।
• **परिचालन व्यवधान:** वेबसाइट क्रैश होना, सिस्टम डाउनटाइम और व्यवसाय संचालन में असमर्थता।
• **कानूनी और नियामक दंड:** ग्राहक डेटा की सुरक्षा में विफलता के लिए जुर्माना और अन्य कानूनी परिणाम।

खतरों को रोकें:

Prevent threats:

हम निम्नलिखित तरीकों से निम्नलिखित ई-कॉमर्स खतरों को रोक सकते हैं:

• **एंटी-मैलवेयर:** हम अपने सभी कंप्यूटर सिस्टम पर एंटी-मैलवेयर और एंटी-वायरस सॉफ़्टवेयर लगा सकते हैं ताकि हम इन स्थितियों को होने से रोक सकें। एंटी-मैलवेयर और एंटी-वायरस सॉफ़्टवेयर सभी प्रकार के मैलवेयर और वायरस को हमारे कंप्यूटर के डेटा को संक्रमित करने से रोकते हैं।

• **HTTPS:** HTTPS वेबसाइट डेटा को किसी भी प्रकार के डिजिटल हमले से सुरक्षित रखने में मदद करता है। SSL और HTTPS उपयोगकर्ताओं के सभी डेटा को एन्क्रिप्ट करते हैं, जिसे हैकर्स के लिए क्रैक करना मुश्किल होता है।

• **भुगतान गेटवे:** हम ई-कॉमर्स वेबसाइटों पर उपयोग किए जाने वाले भुगतान गेटवे को सुरक्षित कर सकते हैं, जिसमें किसी भी उपयोगकर्ता की वित्तीय साख को लीक करने के खिलाफ बहुत उच्च सुरक्षा और सख्त नीतियां हैं।

ई-कॉमर्स में प्रौद्योगिकी समाधान

Technology solutions in e-commerce

ई-कॉमर्स में तकनीकी समाधानों में वैयक्तिकरण और चैटबॉट्स के लिए आर्टिफिशियल इंटेलिजेंस (एआई), इमर्सिव अनुभवों के लिए ऑगमेंटेड रियलिटी (एआर)/वर्चुअल रियलिटी (वीआर), एकीकृत

ग्राहक यात्राओं के लिए ओमनीचैनल प्लेटफ़ॉर्म, सुरक्षित भुगतान गेटवे और ग्राहक अंतर्दृष्टि प्राप्त करने और संचालन को अनुकूलित करने के लिए डेटा एनालिटिक्स शामिल हैं। अन्य समाधान इन्वेंट्री और आपूर्ति श्रृंखला प्रबंधन, मोबाइल कॉमर्स और सुरक्षित लेनदेन के लिए ब्लॉकचेन तकनीक पर केंद्रित हैं।

ग्राहक अनुभव और जुड़ाव प्रौद्योगिकियां

Customer Experience & Engagement Technologies

• **एआई-संचालित वैयक्तिकरण:**
एआई एल्गोरिदम ग्राहक डेटा का विश्लेषण करके वैयक्तिकृत उत्पाद अनुशंसाएँ, अनुकूलित मार्केटिंग और अनुकूलित खरीदारी अनुभव प्रदान करते हैं।

• **एआई चैटबॉट:**
ये बॉट ग्राहक संचार को बेहतर बनाते हैं, तत्काल सहायता प्रदान करते हैं और कार्यों को स्वचालित करते हैं, जिससे ग्राहक यात्रा अधिक कुशल और संतोषजनक हो जाती है।

• **संवर्धित वास्तविकता (एआर) और आभासी वास्तविकता (वीआर):**
एआर ग्राहकों को अपने वातावरण में उत्पादों की कल्पना करने की अनुमति देता है (उदाहरण के लिए, फर्नीचर को आभासी रूप से रखना), जबकि वीआर पूरी तरह से इमर्सिव अनुभव प्रदान करता है, जिससे खरीदारी की अनिश्चितता और रिटर्न कम करने में मदद मिलती है।

• **वॉयस कॉमर्स:**
स्मार्ट डिवाइस और वॉयस असिस्टेंट ग्राहकों को वॉयस कमांड के माध्यम से हाथों से मुक्त खरीदारी करने की अनुमति देते हैं, जिससे सुविधा का एक स्तर बढ़ जाता है।

• **ओमनीचैनल उपस्थिति:**
ये समाधान वेब और मोबाइल से लेकर सोशल मीडिया तक, सभी ग्राहक संपर्क बिंदुओं पर एक सुसंगत और निर्बाध खरीदारी अनुभव प्रदान करते हैं।

परिचालन और प्रबंधन प्रौद्योगिकियां
Operational & Management Technologies

• **ई-कॉमर्स प्लेटफ़ॉर्म:**
शॉपिफ़ाई या वूकॉमर्स जैसे प्लेटफ़ॉर्म ऑनलाइन स्टोर बनाने और प्रबंधित करने के लिए आधारभूत संरचना प्रदान करते हैं, जिसमें वेबसाइट विकास, उत्पाद प्रबंधन और बिक्री शामिल है।

• **इन्वेंट्री और आपूर्ति श्रृंखला प्रबंधन:**
ऐसे समाधान जो एंटरप्राइज़ रिसोर्स प्लानिंग (ईआरपी) सॉफ़्टवेयर के साथ एकीकृत होते हैं, इन्वेंट्री स्तरों का प्रबंधन करते हैं, और आपूर्ति श्रृंखला संचालन को अनुकूलित करने के लिए तृतीय-पक्ष लॉजिस्टिक्स प्रदाताओं से जुड़ते हैं।

• **डेटा एनालिटिक्स:**
ग्राहक डेटा, वेबसाइट ट्रैफ़िक और बिक्री प्रदर्शन को एकत्रित और विश्लेषण करने के लिए उपकरण, ताकि जानकारी प्राप्त की जा सके,

मार्केटिंग प्रयासों को अनुकूलित किया जा सके और परिचालन दक्षता में सुधार किया जा सके।

भुगतान एवं सुरक्षा प्रौद्योगिकियाँ

Payment & Security Technologies

• सुरक्षित भुगतान गेटवे:

क्रेडिट/डेबिट कार्ड, नेट बैंकिंग, डिजिटल वॉलेट और अन्य इलेक्ट्रॉनिक धन हस्तांतरण के माध्यम से ऑनलाइन भुगतान संसाधित करने के लिए आवश्यक।

• ब्लॉकचेन तकनीक:

लेनदेन के लिए बेहतर पारदर्शिता और सुरक्षा प्रदान करती है, जिससे ऑनलाइन बिक्री प्रक्रियाएँ अधिक विश्वसनीय और सत्यापन योग्य बनती हैं।

संचार चैनल को सुरक्षित करना

Securing the Communication Channel

• HTTPS/SSL/TLS:

यह तकनीक डेटा को एन्क्रिप्ट करती है, जिससे ग्राहक के ब्राउज़र और ई-कॉमर्स सर्वर के बीच डेटा की गोपनीयता और अखंडता सुनिश्चित होती है।

• SSL/TLS प्रमाणपत्र:

वेबसाइटें HTTPS को सक्षम करने, वेबसाइट की पहचान सत्यापित करने और ऑनलाइन लेनदेन के दौरान प्रेषित डेटा को सुरक्षित करने के लिए इनका उपयोग करती हैं।

• **VPN (वर्चुअल प्राइवेट नेटवर्क):**
VPN डेटा ट्रांसमिशन के लिए एक सुरक्षित, एन्क्रिप्टेड सुरंग बनाते हैं, जो सुरक्षा प्रदान करते हैं, खासकर सार्वजनिक वाई-फाई का उपयोग करते समय।

खतरों से सुरक्षा के लिए
• **फ़ायरवॉल:**
ये एक अवरोधक के रूप में कार्य करते हैं, नेटवर्क एक्सेस को नियंत्रित करते हैं और अनधिकृत उपयोगकर्ताओं को सिस्टम तक पहुँचने से रोकते हैं।

• **एंटी-वायरस और एंटी-स्पाइवेयर सॉफ़्टवेयर:**
ये उपकरण दुर्भावनापूर्ण कोड और सिस्टम से समझौता करने वाले सुरक्षा जोखिमों का पता लगाते हैं, उन्हें हटाते हैं और रोकते हैं।

• **घुसपैठ रोकथाम प्रणाली (IPS):**
ये स्वचालित रूप से नेटवर्क और ब्राउज़र हमलों का पता लगाते हैं और उन्हें रोकते हैं, जिससे एप्लिकेशन में कमजोरियों से सुरक्षा मिलती है।

ई-कॉमर्स में तकनीकी समाधान) नेटवर्क की सुरक्षा और सर्वर व क्लाइंट की सुरक्षा)

Technology Solution In E-Commerce) Protecting Network And Protecting Server And Client)

नेटवर्क के लिए:

- **SSL/TLS एन्क्रिप्शन:**

भुगतान विवरण जैसे संवेदनशील डेटा को इंटरसेप्शन से बचाने के लिए, सर्वर और क्लाइंट के ब्राउज़र के बीच कनेक्शन को एन्क्रिप्ट करने के लिए एक SSL प्रमाणपत्र स्थापित करें, जिसे HTTPS द्वारा दर्शाया जाता है।

- **फ़ायरवॉल:**

दुर्भावनापूर्ण ट्रैफ़िक को रोकने, SQL इंजेक्शन और क्रॉस-साइट स्क्रिप्टिंग (XSS) जैसे खतरों का पता लगाने और नेटवर्क एक्सेस को नियंत्रित करने के लिए हार्डवेयर और सॉफ़्टवेयर दोनों फ़ायरवॉल तैनात करें।

सर्वर के लिए:

- **नियमित सुरक्षा अपडेट:**

सुनिश्चित करें कि सभी सर्वर सॉफ़्टवेयर और ऑपरेटिंग सिस्टम नियमित रूप से उन कमज़ोरियों को दूर करने के लिए अपडेट किए जाते हैं जिनका हैकर फायदा उठा सकते हैं।

• **डेटा एन्क्रिप्शन और टोकनाइज़ेशन:**
क्रेडिट कार्ड की जानकारी जैसे संवेदनशील ग्राहक डेटा को एन्क्रिप्ट करें, और वास्तविक डेटा को विशिष्ट कोड से बदलकर एक्सपोज़र को कम करने के लिए टोकनाइज़ेशन का उपयोग करें।

• **PCI अनुपालन:**
सुनिश्चित करें कि आपकी वेबसाइट क्रेडिट कार्ड की जानकारी के सुरक्षित संचालन के लिए भुगतान कार्ड उद्योग डेटा सुरक्षा मानक (PCI DSS) का पालन करती है।

ग्राहकों (और उपयोगकर्ताओं) के लिए

• **बहु-कारक प्रमाणीकरण (MFA):**
उपयोगकर्ता खातों के लिए MFA लागू करें, जिससे खातों तक पहुँचने के लिए कई प्रकार के सत्यापन (जैसे पासवर्ड और वन-टाइम पासकोड) की आवश्यकता होगी, जिससे सुरक्षा में उल्लेखनीय वृद्धि होगी।

• **AI-संचालित ख़तरा पहचान:**
कृत्रिम बुद्धिमत्ता (AI) और मशीन लर्निंग (ML) का उपयोग करके वास्तविक समय में ख़तरों का पता लगाएँ और उनका जवाब दें, जिससे संदिग्ध गतिविधि पर निरंतर निगरानी हो।

• **उपयोगकर्ता जागरूकता:**
मानव-कारक-संबंधी सुरक्षा उल्लंघनों के जोखिम को कम करने के लिए मज़बूत पासवर्ड का उपयोग करने और संवेदनशील जानकारी साझा न करने जैसी सर्वोत्तम प्रथाओं के बारे में ग्राहकों को शिक्षित करें।

• **सुरक्षित भुगतान गेटवे:**

Stripe या Square जैसे प्रतिष्ठित, सुरक्षित भुगतान गेटवे के साथ एकीकृत करें जो एन्क्रिप्टेड और PCI-अनुपालन तरीके से लेनदेन को संभालते हैं।