International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

A Comprehensive Exploration of Privacy and Security Mechanisms in E-commerce

Varsha Laad [1]
Research Scholer
Department of Computer Science
Dr. A.P.J. Abdul Kalam University, Indore, India
Jainvarsha05@gmail.com

Dr. Atul Duttatrya Newase[2]
Research Supervisor
Department of Computer Science
Dr. A.P.J. Abdul Kalam University, Indore, India
dr.atulnewase@gmail.com

Abstract: This research is all about making online shopping, or e-commerce, safer. We know that buying and selling things on the internet is easy, but we need to make sure our information stays safe. The study looks at the problems we face, like attacks that try to make websites stop working, unauthorized access to our information, and stealing or fraud. It talks about how important it is to have strong security measures to deal with these risks. It suggests different safety measures like improving how websites talk to each other using SSL/TLS, using strong encryption to protect user information, adding an extra layer of verification (Two-Factor Authentication), and making sure online transactions are secure. It also looks at protecting against specific types of attacks like SQL injection, which is when unauthorized individuals try to mess with a website's database. The study talks about how important it is for online stores to have clear privacy rules, let people shop without giving away too much personal information, and make sure payments are safe. It wants to give practical advice to online stores to make their privacy and security better. The research knows that security problems keep changing, so it says online stores should keep updating how they protect themselves. The primary inquiry it seeks to address is how to make the e-commerce experience safer for all users.

Keywords : E-commerce security, Online shopping safety, Cybersecurity in e-commerce, E-commerce safety protocols, Online payment security, Theft and fraud in online shopping.

I. INTRODUCTION

The internet lets us buy and sell things easily, but we need to make sure our information stays safe. Online business, known as e-commerce, has become really popular, but there's a big worry about safety. If security fails, it can lead to money problems. Even though we use tools like firewalls to improve safety, there are still challenges. E-commerce has changed how businesses and customers interact, offering convenience and lots of choices. But, security and privacy issues are causing trouble. Fixing these problems is super important to keep things going well. One problem is telling if someone is real or a computer during online transactions. Even though we have tools like CAPTCHA, researchers are working on better ways to make things more secure.

This research is all about making e-commerce safer. It looks at the problems, how breaches affect customer trust, and suggests ways to protect your data. The goal is to give helpful ideas for online stores to create a safe and trustworthy place, making things better for both shops and shoppers. As technology and the internet grow, more people are buying and selling things online. E-commerce, done through websites and apps, is convenient and lets us shop globally. But, we worry about our info being safe. Online stores keep a lot of important data, making them targets for hackers. Security is really important to stop money loss, identity theft, and damage to a store's reputation. To fix these issues, stores use tricks like encryption, privacy rules, secure login, and regular security checks. For companies in e-commerce, keeping your info safe is a big deal. There are rules, like the Payment Card Industry Data Security Standard (PCI DSS), to handle credit card info safely. Also, they use things like SSL/TLS to protect data during online buying. By using these tricks, online stores can make their systems safer, protect customer info, and keep trust in the online marketplace.

To keep an online store safe, it's important to know about possible threats. There are three main types of attacks:

1. Denial of Service (DoS): This tries to make a computer or system stop working by sending too many requests or exploiting problems. Traditional DoS floods a system with traffic, while Distributed Denial of Service (DDoS) involves many devices working together. DDoS can target network bandwidth, use up server power, or find problems in the application layer.

2. Unauthorized Access: This is when someone gets into a system without permission. It can lead to theft, fraud, and other problems. Two main types are spamming and viruses.

3. Theft and Fraud: Unauthorized access can lead to stealing sensitive info or doing fake activities. Spamming is sending unwanted commercial emails, and viruses, like worms and Trojan Horses, can do bad things and trick users. To stop these threats, it's important to use security measures and stay alert for possible attacks.

Unauthorized access in cybersecurity means cyberattacks without permission. These attacks aim to get into systems, steal important data, disrupt work, or cause harm by finding weaknesses in computer systems, networks, or apps. Attackers use different methods, like guessing passwords, phishing, keylogging, or malicious software, to get in and maybe hurt the security of online stores.0

This research looks at the challenges of e-commerce, mainly focusing on security and privacy issues. It wants to understand how breaches and privacy worries affect how much customers trust online stores. The goal is to find ways to protect your info better, like using encryption during storage and transmission. It also checks how privacy policies help users know more about how data is collected and used. It looks at things like disguise and anonymity in online shopping and checks if choices like two-factor authentication make accounts more secure. The research also looks at how to keep your money info safe during online payments.

This study suggests doing regular checks and tests to fix any problems in online stores. It also looks at using advanced tools to prevent fraud and how to keep your data safe through encryption, access controls, and backups. The main aim is to give practical advice to online stores to make their privacy and security better based on what's found in the study. The research on e-commerce privacy and security is super important for making customers trust online stores more. If online stores use strong security, it can help people feel safer about their personal and money info, making them more likely to shop online. The study wants to fix security problems, like fraud and data breaches, to help online stores avoid losing money and a good reputation. Knowing that security issues change, the research says stores need to update how they protect themselves. The big question it tries to answer is how to make online shopping safer. The title, " A Comprehensive Exploration of Privacy and Security Mechanisms in E-commerce" shows it's all about making online stores a safe and trustworthy place for everyone.

II. LITERATURE REVIEW

The literature review is like the groundwork for our study. It helps us understand what research has already been done, guiding us in designing our study and choosing the right tools. We look at past reports, articles, and books to get a solid grasp of the topic. Our study is all about e-commerce, buying and selling stuff online. The internet is a big player here. The review aims to dig into issues like privacy and security challenges, why the internet is crucial, how e-commerce is doing in India, and the good and not-so-good sides of security measures. We'll explore various studies to learn more about these aspects and boost our understanding of e-commerce technology.

David Chaum, in 1985, introduced smartcards [1]. These are like small, handy computers that can store your ID details, money matters, medical records, and more. Because all your info is on the card, it makes doing more complicated transactions at places like stores easier. It also helps in keeping your personal information from being stored in one central place. Digital cash and networked payments, another idea from Chaum, let you buy things online without telling anyone about your purchases or who you are. This has made small payments, like paying for individual newspaper articles or using services like PayPal, really popular and successful. Another way to stay safe on the internet, mentioned by Chaum, is using digital watermarking technology. It's like a hidden label for electronic things, such as pictures or audio, that can't be easily removed, copied, or faked. The label is usually subtle or hard to notice. Digital cash and networked payments let you buy things online without telling anyone about your purchases or who you are.

W. Rankl and W. Effing, in 1997, explored encryption techniques focused on asymmetric cryptography [2]. They talked about Public Key Infrastructure (PKI) systems, which are considered really safe. These systems are connected with the Secure Socket Layer (SSL) protocol and a banking standard called ANSI X9. PKI often needs a centralized and easily reachable middleman for managing keys, especially for quickly reporting revoked key-pairs. A common use of PKI is in digital signatures. These are like electronic signatures that can be used to sign contracts, prove who you are for access, or confirm the legitimacy of an electronic distribution.

In 2001, N. Borisov, I. Goldberg, and D. Wagner discussed the importance for e-commerce sites and consumers to carefully assess security vulnerabilities and potential technical solutions [3]. They emphasized the need to evaluate and address associated risks. The researchers pointed out that achieving full connectivity, security, and ease-of-use simultaneously in a networked application is challenging and often involves trade-offs, requiring some level of sacrifice. For e-commerce merchants, the primary security concern highlighted was keeping web servers' archives of recent orders behind the firewall rather than on the more exposed front-end web servers. This approach helps mitigate potential risks and enhances the overall security of e-commerce systems [3].

In 2016, Palak Gupta and team explored the factors influencing Internet users' trust in e-commerce websites [4]. They found that consumer attitudes towards information quality, trust, privacy, reputation, and security significantly impact this trust. Privacy and security emerge as major concerns for both customers and e-commerce sites. Privacy involves controlling personal data, while security deals with preventing unauthorized access to data. Information security becomes crucial for efficient online payment transactions. E-commerce security aims to protect assets from unauthorized access, destruction, alteration, or use, focusing on dimensions like Integrity, Privacy, Non-repudiation, Authenticity, Confidentiality, and Availability. The study reveals that consumer loyalty is closely linked to trust in a website, impacting purchasing behavior. Trust not only influences buying intentions but also affects the cost, preference, and frequency of visits, directly impacting a consumer's profitability. Customer-perceived security in handling personal data strongly influences their trust in the internet. The study concludes that achieving a delicate balance of privacy, trust, and security is essential for successful and measurable e-commerce transactions. Encryption, protection, verification, and authentication mechanisms play a significant role in shaping perceptions of security [4].

In 2017, S. Sridhar and colleagues explored electronic commerce as a modern business method aimed at meeting the needs of organizations, merchants, and commerce. The primary goals include reducing costs and enhancing the quality, services, and delivery speed associated with buying and selling information, products, and services over computer networks. Electronic Data Interchange (EDI), a reliable method for electronic transactions through computer-to-computer communication, is often used in conjunction with just-in-time (JIT) manufacturing methods. Over the years, EDI and email have been key players in facilitating electronic transactions. E-commerce is broadly defined as the purchase or sale of goods or services over the internet. The scope of electronic commerce extends to various technologies and practices, including mobile commerce, electronic funds transfer, supply chain management, Internet marketing, online transaction processing, electronic data exchange (EDI), inventory management systems, and automated data gathering systems [5].

In 2005, Sengupta and team noted the rapid expansion of electronic commerce, attributing it to the convergence of various technologies. The surge in e-commerce is not solely driven by advancements in computer technology but is also influenced by the swift growth of communication networks and the development of sophisticated software. Together, these factors have significantly transformed the landscape of business operations [6].

In 2009, Theresa A. Kraft delved into the relationship between security and the use of Electronic Commerce (E-Commerce) [7]. The common belief is that robust security builds confidence, subsequently driving the increased adoption of E-Commerce. Kraft's study focused on recent market developments in E-Businesses, emphasizing the pivotal role of E-Commerce in the retail industry. The research further explored contemporary E-Commerce practices and trends, particularly highlighting privacy and security concerns. The primary worry revolved around how information exchanges are managed and the potential impact on consumers' privacy. Various privacy concerns were discussed, presenting arguments both for and against these issues. Legal aspects related to privacy concerns were also addressed, evaluating methodologies and providing recommendations for potential solutions. A central concern highlighted in the study is the need to secure users' privacy while conducting electronic business. The study underscored the critical role of security in ensuring the future success of E-Commerce, emphasizing its increasing importance in the global E-Commerce environment [7].

In 2016, Sangeetha M K and Prof. Dr. Suchitra R explored E-commerce Security as a crucial element within the broader Information Security framework [8]. This specialized security focuses on components that specifically impact E-commerce, including Computer Security and Data Security. E-commerce security stands out as it directly affects end customers in their daily financial transactions with businesses. The primary goal of E-commerce security is to safeguard assets against unauthorized access, use, modification, or destruction. Key dimensions of E-commerce security include Integrity, Non-repudiation, Authenticity, Confidentiality, Privacy, and Availability. While E-commerce presents significant opportunities for the banking industry, it also introduces new risks and vulnerabilities, particularly related to internet security concerns. Defining E-commerce security remains challenging due to ongoing technological advancements. The paper provides an overview of E-commerce security, delving into the steps of online shopping, the role of security in E-commerce, various security issues, and guidelines for secure online shopping [8].

In 2008, Hui Lei et al. introduced the Dynamic Distributed Trust Model (DDTM), a general-purpose and application-independent trust model focused on maintaining trust between entities that may never meet [12]. The DDTM aims to create a flexible and distributed Internet-based access control system. The model is explored in the context of digital content delivery, emphasizing operations like initialization, validation, upgrade, degradation, and removal. The Trust Delegation Tree (TDT) framework is employed for developing trust relationships, with mechanisms for node removal and blacklist management. The research lays a foundation for critical trust frameworks in e-Commerce and other Internet-based applications. Similarly, Zhiming QU et al. in 2008 investigated the application of parameter modulation in E-Commerce security based on chaotic encryption [9]. The study addresses the need for network security, market requirements, risks, and technological solutions. A systematic chaotic encryption method is presented, employing a discrete chaotic structure to demonstrate the confidentiality of the encryption process. The research explores the chaotic control system of encryption in E-commerce using chaos theory, emphasizing the unique randomness and sensitivity of chaotic encryption. The adoption of high-dimensional chaotic approaches is suggested to enhance security efficiency, providing a promising avenue for improving enterprise security strategies [9].

In 2016, Patro, Padhy, and Panigrahi explored security issues in E-commerce and proposed solutions. E-commerce involves electronic buying and selling, with various business connections like B2B, B2C, C2C, and C2B. It encompasses processes such as sourcing, transactions, payment processing, and customer service. E-commerce security, crucial for protecting assets from unauthorized access, alteration, or destruction, includes dimensions like Integrity, Non-repudiation, Authenticity, Confidentiality, Privacy, and Availability. Despite offering opportunities for the banking industry, E-commerce introduces challenges like security threats and hacking, requiring both managerial and technical solutions. The article provides an overview of E-commerce security, discusses order placement methods, outlines security goals, identifies challenges, and offers advice for secure online shopping. It emphasizes that E-commerce includes any transaction conducted solely through electronic means, not just buying and selling goods on the internet [10].

III. METHODOLOGY

In this section various steps and processes necessary to improve the privacy and security aspects of e-commerce technologies given in details. The project involves five crucial steps: Research Design, Data Collection, Data Analysis, Mechanism Evaluation, and Results. This systematic approach is designed to enhance the project's effectiveness and generate meaningful outcomes.

1. Secure Sockets Layer/Transport Layer Security (SSL/TLS): This section focuses on improving the security of online communication between web browsers and e-commerce websites using SSL/TLS protocols. It's like adding a digital bodyguard to make sure sensitive information, such as customer details, transactions, and logins, is well-protected during transmission. To implement SSL/TLS, the first step is choosing a reputable Certificate Authority (CA). This CA issues a digital certificate that acts as a virtual ID card for the website, confirming its legitimacy. Following the CA's guidelines, we prove that we own the website, and once verified, the CA provides us with the SSL/TLS certificate.

With the certificate in hand, the next task is configuring the web server hosting the e-commerce site. This involves creating a certificate signing request, submitting it to the CA, and installing the certificate on the server. Ensuring the website uses HTTPS is a key indicator of a secure connection. Looking into the future, SSL/TLS protocols are expected to evolve. The focus will be on adopting even stronger encryption techniques, like post-quantum cryptography, to stay ahead of emerging cyber threats. Additionally, there will be an emphasis on forward secrecy, ensuring that even if future keys are compromised, past communications remain secure. SSL/TLS certificates play a crucial role in establishing trust between web browsers and e-commerce websites. In the future, improvements in the authentication process will enable users to confidently verify the authenticity of the websites they visit, reducing the risk of falling victim to cyber-attacks such as phishing.

These protocols not only protect against potential middlemen attempting to intercept data but also pave the way for additional security measures. Ongoing advancements will continue to minimize the risk of data interception and unauthorized access during transmission, contributing to increased user trust and the seamless completion of secure transactions.

2. Using Strong Encryption: In our e-commerce project, we prioritize the protection of sensitive user information by implementing the robust AES-256 encryption algorithm. This begins with a thorough analysis of the specific security requirements, identifying types of data, such as personal details, payment information, and order summaries, that demand protection. The selection of the AES-256 encryption algorithm stems from its recognition as a widely trusted and secure option, aligning seamlessly with industry standards. To maintain the confidentiality and integrity of the encryption keys, a comprehensive key management strategy is developed, employing techniques like key rotation, segregation of duties, and strict access controls.

During data transit between clients and servers, secure communication protocols like TLS or SSL are implemented to encrypt sensitive data. Similarly, when data is at rest in databases or file systems, AES-256 encryption is applied, using encryption libraries and frameworks within our development environment. For secure key exchange during encryption, industry-standard protocols such as Diffie-Hellman or PKI are employed, ensuring a secure exchange of encryption keys. Regular security audits and penetration testing are conducted to evaluate the robustness of the encryption implementation, identifying vulnerabilities and weaknesses. Implementing strong encryption measures like AES-256 brings several advantages. It enhances overall data security, demonstrating a commitment to data privacy and compliance with regulations. This, in turn, builds trust and confidence among customers, assuring them that their information is handled securely. Moreover, it minimizes legal and reputational risks and future-proofs our security measures with a known and resilient encryption algorithm. Ultimately, the proper implementation of strong encryption safeguards sensitive user data, maintains regulatory compliance, and establishes trust in our e-commerce platform.

3. Two-Factor Authentication: The standard password protection falls short in the face of evolving threats, making Two-Factor Authentication (2FA) a critical player in securing e-commerce websites. The method involves a second layer of verification, such as facial recognition or one-time passwords, providing an additional barrier against unauthorized access.

2FA utilizes different types of tokens for verification, including knowledge-based (PINs, secret questions), physical objects (OTP on mobile or email), and biometric data (fingerprint, retina scan). This multi-factor authentication ensures a higher level of security, where breaching one layer doesn't compromise the entire system. Importance of 2FA mentioned below:

A. Extra Security Level: Enhances overall security by preventing unauthorized access to critical information.

B. Mobile-Friendly: A seamless process for users, especially on mobile devices, contributing to a smoother authentication experience.

C. Boosted Trust: Instills confidence in customers, as they can reset preferences securely, fostering a sense of reliability.

D. User-Friendly: Requires minimal effort from consumers, promoting ease of use and cost-effectiveness.

***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

E. Secure Payment Gateway: Securing financial transactions is a critical aspect of e-commerce. Payment gateways play a pivotal role in ensuring secure processing. Measures like PCI compliance and 3-D Secure implementation contribute to robust payment security.

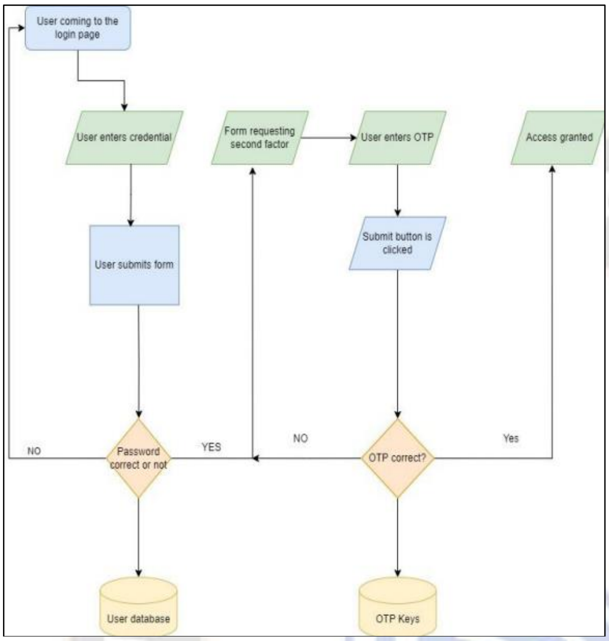

Fig. 1 Two factor Authentication

4. Security Architecture of Payment Gateway: A secure server utilizing SSL provides encrypted online transactions, ensuring customer data remains confidential. The payment gateway acts as a secure intermediary between the customer, the bank, and the merchant, processing transactions securely.

WAF acts as a shield against malicious attacks on web applications. By filtering and visualizing HTTP traffic, it protects against cross-site scripting, cross-site forgery, file inclusion, and SQL injection. WAF can be implemented in following ways:

A. Network-based WAF: Hardware-based, offering robust security but at a higher cost.

B. Host-based WAF: Less expensive, integrated with software applications, but complex to implement.

C. Cloud-Based WAF: Easy implementation, cost-efficient, and continuously protects against evolving threats, but relies on third-party responsibility.

Gatekeeper Function acts as an application layer security solution, protecting against various threats. Comprehensive Protection safeguards against malware, hackers, bots, and other threats, especially crucial for e-commerce stores. In conclusion, the integration of 2FA, secure payment gateways, and WAF forms a comprehensive security approach, fortifying e-commerce platforms against evolving cyber threats and instilling confidence in users.

5. Protection Against SQL Injection: SQL injection is a well-known form of injection attack, poses a significant threat to web applications that utilize SQL databases. As a frequently encountered cyber assault, understanding its workings and implementing robust preventive measures becomes paramount.

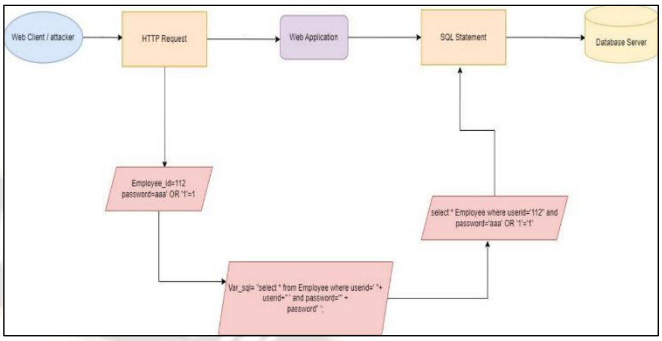
Web Client / attacker
HTTP Request
Web Application
SQL Statement
Database Server
Employee_id=112 password=aaa' OR '1'=1
select * Employee where userid='112' and password='aaa' OR '1'='1'
Var_sql= "select * from Employee where userid=' "+ userid+" ' and password='" + password" ';

Fig. 2 SQL Injection

SQL injection leverages vulnerabilities in web applications, primarily due to inadequate input validation. Attackers strategically insert malicious SQL statements into input fields, aiming to exploit the system and gain unauthorized access to the database. For instance, in an admin login scenario, an attacker manipulates the input by injecting SQL statements like "OR 1=1 --" in the username field and "admin" in the password field effectively bypassing password checks and gaining unauthorized access. While defensive coding is a fundamental practice, additional tools and techniques are vital for thwarting SQL injection attacks. Several tools assist developers in preventing these attacks:

A. JDBC-Checker: Originally not designed for SQL injection prevention, it aids in detecting attacks that exploit type mismatching in dynamically-generated query strings.

B. CANDID: This tool, designed for Java-based web applications, dynamically extracts the intended query structure from programmer-provided input. By comparing it with the executed query structure, CANDID effectively identifies SQL injection attacks.

C. AMNESIA: A hybrid approach combining static analysis and runtime monitoring, AMNESIA constructs models of permitted query structures during static analysis. In the dynamic phase, it intercepts and verifies queries against these models, blocking unauthorized or malicious queries from accessing the database.

These preventive measures act as guardians of the database castle, enhancing the resilience of web applications against the persistent threat of SQL injection attacks. Implementing a multi-layered defense strategy is crucial in safeguarding sensitive information and maintaining the integrity of web systems.

6. Conduct Regular Security Audits and Penetration Testing: In the ever-changing world of keeping digital information safe, organizations use two important practices: security audits and penetration testing. A security audit is like a thorough checkup for your computer systems and networks. It involves carefully examining everything to ensure there are no weak points that could be exploited by hackers. It's akin to a detective investigating a crime scene, looking for any clues that might indicate a security problem. On the other hand, penetration testing is like hiring a friendly hacker to try and break into your systems with your permission. These ethical hackers simulate real attacks, helping you find and fix vulnerabilities before malicious actors can exploit them. In simpler terms, security audits and penetration testing are like regular checkups and controlled break-in attempts for your digital "castle," ensuring your information stays safe from potential cyber threats.

7. When Security Audit required: The frequency and number of security audits an organization needs depend on its industry, business demands, corporate structure, and the scope of systems and applications requiring evaluation. Sectors dealing with substantial sensitive information, such as financial institutions and healthcare providers, often conduct audits more frequently due to the heightened need for robust cybersecurity measures.

A. Network Vulnerabilities: During an audit, experts search for any weak points in the network's parts that could be exploited by attackers to gain access to system information and cause harm.

B. Security Control: In this phase, auditors check how well a company's security measures work. They assess if the organization's policies and procedures are effectively implemented to safeguard against potential threats.

C. Software Systems: Auditors test software systems to make sure they work correctly and provide accurate information. They also examine if the right procedures are in place to stop unauthorized access to confidential data. This includes looking into how data is processed, how software is developed, and how computer systems are set up.

8. Secure Authentication and Authorization: In the ever-evolving digital landscape, safeguarding data and resources against unauthorized access is non-negotiable. The linchpin of modern information security systems rests on the robust interplay of authentication and authorization, forming a dynamic duo to ensure that access is granted only to the right individuals or entities for specific tasks within a system.

Authentication serves as the inaugural defense line, confirming the legitimacy of individuals or devices seeking access. Whether through traditional credentials like usernames and passwords or cutting-edge methods such as biometric scans or multi-factor authentication, the goal is to build trust in users' identities. By validating the accuracy of credentials, authentication ensures that only those with permission gain entry.

Once a user's identity is authenticated, the journey continues with authorization—a phase that determines the extent of privileges or access granted. Factors like the user's role, permissions, and the context of access requests are carefully weighed during authorization. It guarantees that authorized users operate within the bounds of their designated rights and responsibilities, enforcing access control policies to prevent unauthorized actions. To bolster the security of authentication and authorization, additional layers come into play. Encryption, secure protocols, and continuous monitoring of user activities contribute to a resilient defense mechanism. Technological advancements, including artificial intelligence and machine learning, are harnessed to detect and mitigate potential threats like unauthorized access attempts and suspicious behaviors.

9. Employ Intrusion Detection and Prevention Systems: In the ever-changing landscape of cyber threats, firewalls alone are insufficient to protect systems from sophisticated attacks. Intrusion Detection and Prevention Systems (IDPS) are the guardians that collaborate with firewalls to monitor and manage network traffic effectively. These systems, comparable to airport security checks, play a crucial role in maintaining a secure digital environment. Following are the types of IDPS:

A. Network-based Intrusion Prevention System (NIPS): Positioned behind firewalls, NIPS actively monitors entire networks, identifying and thwarting malicious traffic by matching patterns with known attack signatures. It adds an extra layer of defense against network-based attacks.

B. Wireless Intrusion Prevention System (WIPS): Tailored for wireless networks, WIPS scrutinizes wireless networking protocols to detect and prevent unauthorized activities. Installed strategically within wireless networks, WIPS focuses on wireless-specific protocols for specialized security measures.

C. Network Behavior Analysis (NBA) System: Unlike NIPS, NBA systems identify risks by analyzing unusual traffic patterns, pointing to policy violations, malware-driven attacks, or DDoS incidents. Placed at key intersections within internal networks, NBA systems monitor and reduce security concerns.

D. Host-based Intrusion Prevention System (HIPS): Deployed on specific hosts, HIPS monitors active processes, network activity, system logs, and application behavior. This host-level vigilance aims to identify and prevent illegal actions, invasions, or security lapses.

Following are the benefits of IDPS:

A. Threat Detection: Monitors network traffic to identify known attack patterns, anomalous behavior, or signs of intrusion attempts.

B. Incident Response: Provides real-time alerts, enabling swift responses to security incidents and mitigating potential damage.

C. Prevention: Actively blocks or mitigates detected threats, preventing compromise of network resources or sensitive data.

D. Compliance: Helps organizations meet regulatory requirements by offering proactive security solutions and generating audit logs.

IV. RESULT AND ANALYSIS

The registration page, found on websites or apps, is like a digital form where users can create an account or join a service, platform, or website. It serves as a way to gather important details from users to set up a special identity for them in the system. Once users have registered, they can

***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

use the login page to access their accounts. The login page takes in information provided by the user, such as a username and password. Its main job is to collect these login details and check if they match the information stored during the registration process. In essence, it's like a virtual gatekeeper, ensuring that only those with the correct login credentials can enter and access their personalized accounts. This two-step process of registration and login is a common way for digital platforms to manage user identities and provide secure access to personalized services.

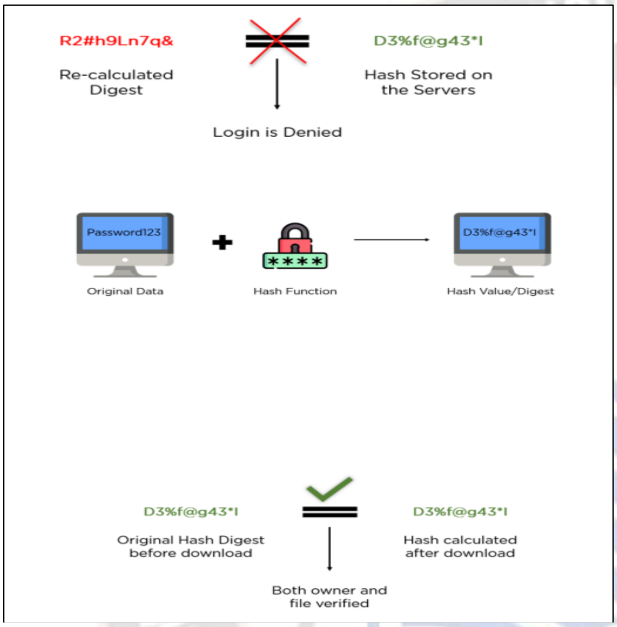

Fig 3. Implementation workflow of the SHA256 algorithm

The above flow diagram illustrates how the algorithm functions. Initially, it receives the initial data as input from the user. Subsequently, the algorithm generates a hash value or digest, which is then stored on the server. During the verification process using a different key, the encrypted string is transformed back into the original script, and both values are compared for authentication.

V. DISCUSSION AND RECOMENDATION

The company discusses how well their security system works. They've done a good job with things like encryption and monitoring to keep customer data safe from cyber threats. Although there were some challenges during the setup, like coordinating with different teams and keeping up with changing cyber threats, they've learned from it. The company stresses the importance of everyone understanding the role they play in keeping the platform secure. They're open to feedback from customers and experts to keep making things better. The security system has made customers trust the platform more, and it has also reduced the risk of data breaches. They acknowledge that even though they've achieved a lot, they know the world of cybersecurity is always changing. They see their success as a starting point for more improvements, using what they've learned to stay ahead of new threats and challenges.

The suggestions in this section aim to make the platform's security even stronger. It's like giving the platform a shield against new and changing cyber threats. The ideas include keeping up with the latest security technology, using smart tools to recognize and stop tricky threats, and regularly checking the platform's security with the help of experts. There's also a plan for responding quickly if there's a security issue, and everyone involved will get training to recognize and avoid common tricks used by cyber attackers. The platform will work together with others in the cybersecurity community to share information about potential threats and learn from each other's experiences. They'll also do practice exercises to test and improve their defence. The goal is to keep learning, stay prepared, and always be ready to protect the platform and its users from cyber risks.

VI. CONCLUSION

In conclusion, our efforts to make our e-commerce platform super secure have been a success. We aimed to ensure the safety of customer data from online threats. We implemented a strong strategy with advanced security measures, acting like a powerful shield to fend off potential dangers in the online shopping world. We made sure our customer data was like a secret code that only the right people could understand, making it tough for unauthorized folks to get in. We also kept a close eye on our system, checking for anything suspicious and fixing it right away to keep our e-commerce platform running smoothly. Regular checkups and improvements in our security system, like adding extra locks, not only restored trust among our loyal customers but also boosted our e-commerce platform's reputation.

In the end, the implementation of our comprehensive security system has solidified our e-commerce platform as a trusted and secure marketplace. The success achieved through vulnerability assessments, encryption, access controls, and staff training demonstrates our commitment to mitigating cyber risks and safeguarding customer data. As we move forward, the durability and success of our e-commerce system depend on continuous monitoring and enhancement of security procedures to adapt to the evolving threat landscape.

References

1. Muzaki, R. A., Briliyant, O. C., Hasditama, M. A., & Ritchi, H. (2020, October).Improving Security of Web-Based Application Using ModSecurity and Reverse Proxy in Web Application Firewall. In 2020 International Workshop on Big Data andInformation Security (IWBIS) (pp. 85-90). IEEE.
2. Nasereddin, M., ALKhamaiseh, A., Qasaimeh, M., & Al-Qassas, R. (2023). A systematic review of detection and prevention techniques of SQL injection attacks.

Information Security Journal: A Global Perspective, 32(4), 252-265..

3. Berrios, J., Mosher, E., Benzo, S., Grajeda, C., & Baggili, I. (2023). Factorizing 2FA:Forensic analysis of two-factor authentication applications. Forensic Science International: Digital Investigation, 45, 301569.
4. Mohamad, M. B., Kanaan, A. G., Aseh, K., Alawi, N. A., Amayreh, K. T., Al Moaiad, Y., ... & El-Ebiary, Y. A. B. (2021, June). Enterprise Problems and Proposed Solutions Using the Concept of E-Commerce. In 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE) (pp. 186- 192) IEEE.
5. Reese, K., Smith, T., Dutson, J., Armknecht, J., Cameron, J., & Seamons, K. (2019).A usability study of five {two-factor} authentication methods. In FifteenthSymposium on Usable Privacy and Security (SOUPS 2019) (pp. 357-370).
6. Li-Xiao Geng, Zhen-Xiang Zeng, Xue-Min Zhang, “Research on PKI-Based E-Commerce Security Mechanism”, IEEE Access,October 2007.
7. Hui Lei, Gholamali C. Shoja “A Distributed Trust Model for e-Commerce Applications” University of Victoria, Victoria, BC, Canada V8W 3P6
8. Delaigle, J-F., C. De Vleeschouwer, and B. Macq. 1996. Digital Watermarking. Proceedingsof the Conference 2659 - Optical Security and Counterfeit Deterrence Techniques : 99-110.
9. Junhong Lian,“Application of Computer Network Security Technology in Electronic Commerce”, IEEE Access, March 2022.
10. Reese, K., Smith, T., Dutson, J., Armknecht, J., Cameron, J., & Seamons, K. (2019). A usability study of five {two-factor} authentication methods. In Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019) (pp. 357-370).