ISSN PRINT 2319 1775 Online 2320 7876

Research paper

 UGC CARE Listed (Group -I) Journal Volume 8, Issue 4, 2019

Ensuring Trust and Safety in Online Trading: A Comprehensive Cyber Security Strategy to Safeguard Financial Transactions and Protect User Privacy

Rajeev Kudari,

Department of Computer Science & Engineering, Programme Co-ordinator BCA (CDOE),

Koneru Lakshmaiah Education Foundation, Green Fields, Vaddeswaram, A.P. – 522302.

Email: krajeev@kluniversity.in

Abstract—

The evolution of internet technologies has revolutionized traditional business services, transitioning many into online platforms. Online trading, serving as a financial hub for share transactions, bids, and product exchanges through computers, plays a pivotal role in this digital transformation. However, the indispensable B2B, B2C, and C2C transactions within online trading are constantly threatened by spyware, malware, hijackers, and intruders. The risk extends to the exposure of trading secrets and portfolios, as network attackers illicitly track the personalized data of business clients. Cybersecurity emerges as a critical domain, providing essential strategies and algorithms to safeguard sensitive data in cyberspace. This paper delves into the cybersecurity issues associated with online trading and outlines the implementation of robust security measures within a key business portal dedicated to market transactions. The discussion encompasses various strategies to address security risks, presenting an approach to secure transactional data in E-Commerce. A comprehensive 3-phased cybersecurity pipeline is proposed to ensure high-end security maintenance for online trading transactions.

Keywords— Cryptography, Encryption, Key, Cookies, Digital Signatures

INTRODUCTION

Cybersecurity represents a strategic ensemble of defensive systems designed to shield computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks [1][2]. The frequency of global security breaches in cyberspace is escalating at an alarming rate, posing significant risks to confidentiality [5]. The early detection and recommendation of risk avoidance strategies are keen interest of Cyber Security [3]. The US

ISSN PRINT 2319 1775 Online 2320 7876

Research paper

 UGC CARE Listed (Group -I) Journal Volume 8, Issue 4, 2019

government introduced Cyber laws to enforce security with a legal framework over cyber space earlier to 2012. The Network Security innovations leaded to discover strong cryptographic environments in protesting business data among open networks. Increased data explosion and vulnerabilities caused by advanced hackers placing many challenges daily upon cyber security framework [6]. The process of buying and selling of things over Internet is referred as E-Commerce activity [7]. The trading now is becoming online in majority of companies to enhance their business borders and increasing the investors [9]. E-commerce is providing a platform for mobile commerce, internet marketing, electronic fund transfer, online transaction processing, automated data collection, legal notaries and electronic fund transfer [4]. As the Internet is unsafe and exploits security breaches, data misuse, frauds and malicious attacks [10]. Cyber Security originated with principles to protect digital electronic systems and data from malicious attacks [11]. The applications involved in business trading must maintain strong authentication, validating rules to support safe transactions among B2B and B2C [12]. Wide range of policies and frameworks developed in cyber security to support trusted business transactions [13]. The advancement in cryptography and Network Security facilitating more advanced digital signatures, cryptographic algorithms and hashing techniques [5]. The modern integration of electronic systems with microprocessors is used to gather data from heterogeneous smart systems, which increases vulnerability in E-Commerce activities [14]. Cyber Security Management offers robust policies encompassing compliance assessment, cyber maturity assessment, data leakage identification, and identity and access management. It is crucial to regularly validate these policies in alignment with the ever-evolving landscape of current business technologies and environments, particularly in the realm of E-Commerce services. This dynamic approach ensures that cybersecurity measures remain effective and adaptive to the continuously changing cybersecurity landscape. [15].

CYBER SECURITY MANAGEMENT

Financial Financial institutions, premier industries, public sector business organizations, and affiliated companies have emerged as primary targets for cyber-attacks. The sheer volume of online transactions across various platforms faces daily security threats. According to US government statistics spanning from 2010 to 2020, the business domain incurred losses totaling around 1.5 billion dollars due to cyber-attacks.

These attacks on business, marketing, and online trading portals can be classified into five

ISSN PRINT 2319 1775 Online 2320 7876

Research paper
 UGC CARE Listed (Group -I) Journal Volume 8, Issue 4, 2019

major categories.

A. Ransom ware & Malware attacks:

The illicit access to sensitive data through hijacking, coupled with the extortion of funds, characterizes a growing threat. Ransomware, a type of malware, encrypts vital databases and applications within organizations, effectively locking files and restricting access to system modules for staff members. Perpetrators then demand payment in exchange for releasing the locks on crucial company data. This not only results in significant disruptions to organizational functioning but also incurs substantial costs for cleaning up networks and restoring normal business operations.

B. End Point Attacks:

The extensive reliance on cloud services is expanding attack surfaces, providing intruders with opportunities to circumvent security measures. Hackers are increasingly focusing on shadow IT services intertwined with company resources, with SaaS and PaaS services offered by cloud servers being prime targets for cyber-attacks. Despite the availability of end-to-end encryption schemes, it remains imperative for cloud providers to consistently update their cybersecurity policies to effectively address evolving security challenges.

C. Phishing Attacks:

Phishing stands out as one of the most cost-effective methods of cyber-attack, strategically attaching malware to trusted services such as email, chatrooms, Dropbox, Slack, Office, and Salesforce. Hackers continually enhance their skills, extending the reach of phishing to encompass social media applications. The potential victims span a wide spectrum, including business customers, stakeholders, B2B, B2C, and various organizations. These attacks range from basic credential stuffing to more sophisticated forms of spam engineering.

D. Third Party/ Supply chain Attacks:

These attacks are prevalent in digital supply chain systems, where company systems interface with third-party service providers. The heightened reliance on external libraries and security patches poses vulnerabilities. In instances where these update providers fall prey to hacking, organizational system configuration files may be redirected to malicious servers, inflicting significant damage on the security architecture of business systems.

ISSN PRINT 2319 1775 Online 2320 7876

Research paper

 UGC CARE Listed (Group -I) Journal Volume 8, Issue 4, 2019

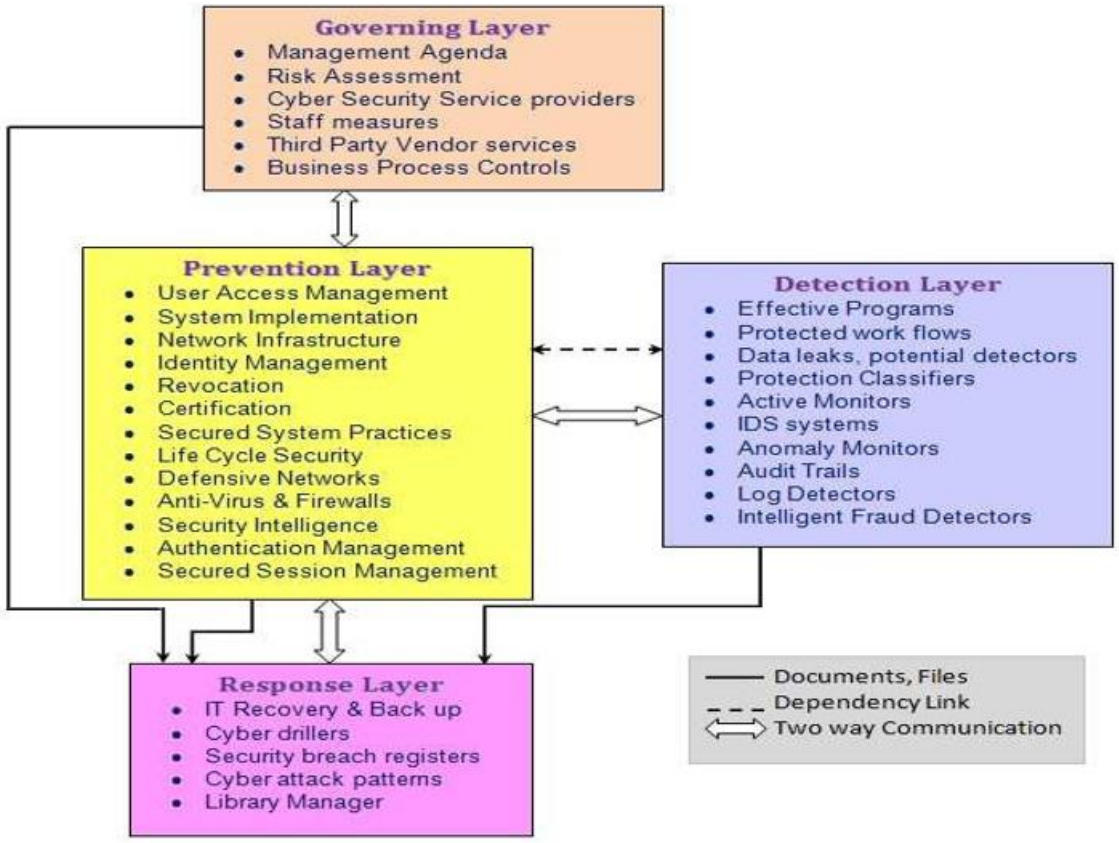

Fig. 1 Cyber Security Management Protocol System

Cyber Security Management Protocol (CSMP) is one solution to reduce cyber-attacks and safe-guard online trading and market transactions. The CSMP architecture framework is shown in figure 1.

Governing Layer:

The management personnel, stakeholders, and administrative team constitute pivotal assets within this layer. Their primary responsibility involves formulating a comprehensive management agenda for the entire organization, with a focus on securing transactions. This group collaborates with cybersecurity professionals who craft security strategies and architectures in accordance with regulatory guidelines, functioning as essential "Cyber Security Providers." The development and management of all business modules and processes, including control layouts, fall under the purview of this layer. This layer oversees the relationships and agreements between the company and trusted third-party groups. Within this layer, the Risk Management authority serves as a sub-module responsible for conducting risk analysis, implementing risk mitigation strategies, and offering risk removal services in

ISSN PRINT 2319 1775 Online 2320 7876

Research paper

 UGC CARE Listed (Group -I) Journal Volume 8, Issue 4, 2019

alignment with industrial standard policies. A dedicated group within the management teams consistently measures the quality of staff and their skills, with a heightened awareness of cybersecurity. The Governing Layer assumes full responsibility for monitoring and controlling the cybersecurity framework within the organization.

Prevention Layer:

At the core of the CSMP protocol, this vital layer plays a crucial role in key activities such as preventing security breaches and safeguarding against sensitive data loss within the organization. User Access Management governs hierarchical-based authentication for company staff, providing a robust system for controlling access. The credential organization empowers high user personalization control over authenticated services. System implementation ensures the organized interaction of secured modules for seamless transaction management. This layer diligently monitors the entire network infrastructure within the company, applying an optimal cybersecurity framework to fortify the organization against potential threats Identity management assumes responsibility for fostering trusted communication between B2C, B2B, and third-party services. Its major activities include certifying digital open systems communication, managing digital signatures, and administering the granting/revoking of privileges over services through secure system practices. This layer meticulously monitors the overall system life cycle security, reinforced by defensive networks, anti-virus measures, and firewall support. It provides security intelligence to activate automated data recovery and authentication log recovery, enhancing secured session management. Operating on the principle of "Prevention is better than curing," this layer supports documentation submitted to the response layer module library management for future surveys.

Detection Layer:

This layer functions as a subordinate to the Prevention layer, actively engaged in tracking security threats across business networks, domain services, and transactions. Employing a suite of effective algorithms and techniques embedded within programs, it excels in detecting cyber-attacks. This layer orchestrates protected workflows with milestone interrogations focused on identifying security loopholes. By organizing Active-Monitors and Anomaly Monitors, it diligently tracks potential threats in system workflows. Additionally, it generates protection classifiers to promptly identify new data leaks and provides support for IDS (Intrusion Detection System) across the entire business network. The layer manages audit trails over

ISSN PRINT 2319 1775 Online 2320 7876

Research paper

 UGC CARE Listed (Group -I) Journal Volume 8, Issue 4, 2019

transactional data, utilizing log detectors to identify any session threats in the active log history. A collection of intelligent fraud detectors, integrated with the latest strategic frameworks, ensures swift identification of cyber-attacks or frauds in real time. All detected security breach activities are meticulously documented and submitted to the "Library Manager" of the Responsive Layer for further analysis and response.

Responsive Layer:

Serving as the linchpin for all layers within the CSMP system, this pivotal layer takes on the responsibility of managing data recovery, data backup, documentation, security breach registers, and cyber-attack patterns. Functioning as the central library for the entire business data organization, it acts as a comprehensive repository. Additionally, it supports specialized tools known as "Cyber Drillers," which continually explore cyber space to gather the latest information about cyber-attacks and their remedies. The Governing layer directly accesses the information repositories within this layer for auditing purposes, ensuring a robust and comprehensive approach to cybersecurity management.

CYBER SECURITY PIPELINE MODEL

Positioned between the customer and the CSMP system of the organization, the proposed three-phased security pipeline model for online trading services acts as a crucial checkpoint. For transactional data to successfully traverse from either the customer or the business organization system, it must navigate through three distinct phases of security.

A. Cryptography Phase

In the initial phase dedicated to handling data from open networks, cryptographic techniques are deployed for the secure transmission and reception of information. Clients submit their credentials and transaction support data through a public key cryptographic mechanism, wherein the client sends two public keys, and the organization maintains a private key to facilitate data exchange using RSA/ECC techniques. This phase is designed to ensure a high degree of security for client-sensitive data in cyber space. In the sending mode, the business organization generates a single public key distributed to specific authenticated clients to receive data from encrypted sources, a process made possible by applying the client's private key.

B. Credentiality Phase

The second phase in pipeline identifies client authentication and request handler identity in business system. Transactions of information distribution between business modules to

ISSN PRINT 2319 1775 Online 2320 7876

Research paper

 UGC CARE Listed (Group -I) Journal Volume 8, Issue 4, 2019

specific clients are safeguarded within the company also. Each client transaction subjected to HMAC to generate unique specific system identity such that only that system can handover incoming client information files by applying HMAC/MD5 technique. The second phase supports a strict one-to-one secured communication among clients and network authenticated system.

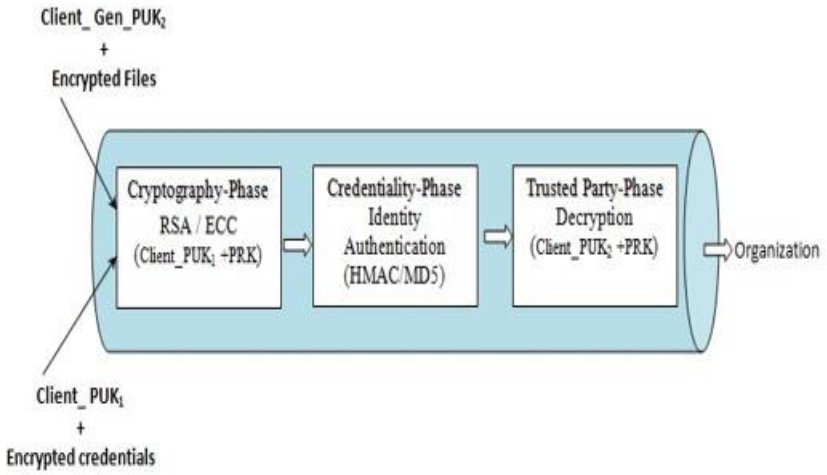

Fig. 2 Three PHASED security pipeline Model

The advantages of proposed security pipeline system are

- Customer credentials benefit from robust RSA 128-bit encryption, providing a formidable defense against potential attacks.
- Details in customer forms for online trading agreements and business dealings undergo encryption. Only the trusted business system can decrypt this information using a combination of Hash function (Authentication) and a private key (Decryption).
- Transaction initiation is contingent upon the successful verification of customer credentials in Phase-1.
- Intruders, hackers, and other malicious actors are effectively thwarted from accessing the original data through the communication channel.
- The customer end is fortified with a highly secure interface, incorporating digital signatures, RSA, and ECC mechanisms for the robust encryption of trading information.
- Even within the company's private business network, information exchange adheres to a one-to-one communication model, exclusively between the customer and the trusted

ISSN PRINT 2319 1775 Online 2320 7876

Research paper

 UGC CARE Listed (Group -I) Journal Volume 8, Issue 4, 2019

entity.

- Information security levels can be systematically enhanced in a hierarchical fashion.
- The three-phase validation system significantly bolsters the cybersecurity of business systems, fortifying services provided to customers through online portals.
- Auctions, bidding, and quotations related to online transactions are exceptionally secured between the customer and the company, thanks to the implementation of this robust security model.

Algorithm for Client to Business Transaction three-phased Security Process

Input:

Client _Transaction_Profile, Public_Keys, Client_Credentials,

BS_PRK, Client_PRKOutput:

Secured receiving of Client_Transaction_Data

Step 1: Submission of client credentials as encrypted file using client publickey (PUK_1) and client private key (PRK)

Step 2: Validation of client credentials by business system using public keyalgorithm with PUK_1

Step 3: Send acknowledgement to client for transaction process initialization.

Step 4: Submission of client transaction data as encrypted file using client public keyPUK_2 and private key PRK_C

Step 5: Decryption of client transaction by business system using PUK2 and privatekey PRK_b

Step 6: Applying HMAC/MD5 to identify trusted third party in business systemnetwork.

Step 7: Sending Authenticated data to third party.

Step 8: Validating received data with HMAC/MD5 as authenticated receiver

Step 9: Acknowledge to Business security system for trusted transaction success Step 10: Stop

CONCLUSIONS

leveraging cryptographic mechanisms, the model encrypts trading transactions, offering customers a trusted channel for transferring crucial business files to authenticated authorities

ISSN PRINT 2319 1775 Online 2320 7876

Research paper

 UGC CARE Listed (Group -I) Journal Volume 8, Issue 4, 2019

and vice versa. The Two-key mechanism enhances security by separately encrypting customer credentials and transaction data as two distinct files, each requiring a corresponding private key for decryption. This dual-key approach significantly fortifies data security, imposing a formidable challenge for hackers. Customers are facilitated with organization-provided application software or a mobile app to seamlessly navigate this 3-phase pipeline security model. Despite the model's provision of highly reliable cybersecurity for online traders, adherence to guidelines is imperative to prevent security breaches. An effective policy involves timed public key generation, wherein a public key remains active for a brief period between the parties involved. Ongoing research endeavors are anticipated to enhance cybersecurity and mitigate security risks in cloud business networks. While cryptographic techniques may marginally increase transaction time, they concurrently deliver heightened security for safeguarding sensitive data among business clients.

REFERENCES

[1] Rammanohardas, "Artificial Intelligence in Cyber Security", Journal of Physics, Conference on Artificial Intelligence and modern applications, 240-ECS Meeting, 2000

[2] Md. Shafiur Rahman, Sajal Halder, U. Kumar Acharjee, "An Efficient Hybrid System for Anomaly Detection in Social Networks", Springer, Article.No:10, Vol.4, DOI: https://doi.org/10.1186/s42400-021-00074-w, 2000.

[3] M. Humayun and M.Niazi, " Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study", Arabian Journal of Science & Engineering, DOI: 10.1007/s13369-019-04319-2, PP: 1245-1250, 2012.

[4] Alex Mathew, "Machine Learning in Cyber-Security Threats", International Conference on IoT Based Control Networks & Intelligent Systems, DPI: 10.2139/ssrn.3769194, 2012.

[5] Anand Shinde, "Introduction to Cyber Security: Guide to the World of Cyber Security", ISBN: 978-1-63781-642-4, Notion-Press, 2002.

[6] S. Arumugam, “A Review on Cyber Security and the Fifth-Generation Cyber Attacks", Journal of Computer Science and Technology, Vol. 12(20, DOI:10.13005/ojcst12.02.04, PP: 50-56, 2013.

[7] Yu[chong Li, Qinghui Liu, "A Comprehensive Review Study of Cyber-Attacks and Cyber Security; Emerging Trends and Recent developments", Elsevier, Science Direct

ISSN PRINT 2319 1775 Online 2320 7876

Research paper

 UGC CARE Listed (Group -I) Journal Volume 8, Issue 4, 2019

Publication, DOI: 10.1016/j.egyr.2021.08.126, pp: 101-108, 2014.

[8] K. Cabaj, Z. Kotulski, B. Ksiezopolski, "Cyber Security: Trends, Issues and Challenges", Springer, EURASIP Journal, Vol. 10, DOI: 10.1186/s13635-018- 0080-0, 2018.

[9] I Agrafiotis, Jason R C Nurse, "A Taxonomy of Cyber-harms: Defining the Impacts of Cyber-Attacks and understanding how they Propagate", Journal of Cyber Security, DOI: doi.org/10.1093/cybsec/tyy006, Vol.4, Issue-1, 2018.

[10] Muhammad Kashif, Sheraz Arshad Malik, "A Systematic Review of Cyber Security and Classification of Attacks in Networks", IJACSA, Vol.9, No.6, PP:201-207,2018

[11] Stallings William, "Cryptography and Network Security", Pearson, ISBN: 978-9332585225, 2017.

[12] Meikang Qiu, K. Thakur, "An Investigation on Cyber Security Threats and Security Models", IEEE- ICCSCC Conference, DOI: 10.1109/CSCloud.2015.71, 2015.

[13] G.J. Ugander and G. Nikhita Reddy, "A Study of Cyber Security Challenges and its Emerging Trends on Latest Technologies", IJCAT, Vol-3, Issue-10, PP: 123-126, 2014.

[14] Nina Godbole, Sunit Belapure, "Cyber Security", ISBN: 978-8-12652-179-1, Wiley-Edition, 2011.

[15] R.A. Kemmerer, "Cyber Security a Comprehensive Study", 25th ICSE Proceedings, ISSN: 0270-5257, May-2003, USA