Smart and Secure Point of Sale Framework with Threat Modeling and Formal Verification

Mona faraj Nasser alwahabi[1] and Shaik Shakeel Ahamad[2]
[1]431204474@s.mu.edu.sa, [1]Monafr00075@gmail.com, [2]ahamadss786@gmail.com [2]s.ahamad@mu.edu.sa
1&2Department of Information Technology, College of Computer and Information Sciences Majmaah University, Al-Majmaah, 11952, Saudi Arabia

Abstract
Existing PoS (Point of Sale) based payment frameworks are vulnerable as the Payment Application's integrity in the smart phone and PoS are compromised, vulnerable to reverse engineering attacks. In addition to these existing PoS (Point of Sale) based payment frameworks do not perform point-to-point encryption and do not ensure communication security. We propose a Smart and Secure PoS (SSPoS) Framework which overcomes these attacks. Our proposed SSPoS framework ensures point-to-point encryption (P2PE), Application hardening and Application wrapping. SSPoS framework overcomes repackaging attacks. SSPoS framework has very less communication and computation cost. SSPoS framework also addresses Heartbleed vulnerability. SSPoS protocol is successfully verified using Burrows–Abadi–Needham (BAN) logic, so it ensures all the security properties. SSPoS is threat modeled and implemented successfully.

Keywords:
Smart and Secure PoS (SSPoS), Smart Point of Sale (SPOS); Burrows–Abadi–Needham (BAN); POS Payment Application (PPA); Point-to-Point encryption (P2PE); Application hardening and Application wrapping

I. Introduction

The huge adaptation of smart phones increased the PoS based payments which attracted the cyber-intruders for sensitive data which includes credit card numbers, Order Information and personal information. No entity in the payment ecosystem is safe. No entity in the payment ecosystem is safe which includes banks, merchants, Payment gateways and insurance companies. Financial institutions need to adhere to the Payment Card Industry Data Security (PCI DSS) standards. Following are the consequences for Non-Compliance with PCISDSS standard.

a) Monetary penalties
b) Legal consequences
c) Damaged Reputation
d) Loss of customers
e) Forensics Audits
f) Payment brand restrictions
g) Brand reputation

So, PCI DSS plays very vital role in banking industry as it reduces the risk of a data breach, protects customer data from fraud and theft, increases customer's trust, reduces the costs, improves employee security awareness, enhances security controls, increases the bank's reputation and protects banks from fines and penalties. PoS systems usually face the same threats and vulnerabilities Faced by computers and operating systems such as Window and Linux. Common attacks on PoS systems are through keylogging Trojans, replaying login and brute force techniques. Existing PoS based mobile payment frameworks do not perform *point-to-point encryption which is very important for merchant based transactions.*

Motivation

The main motivations for this research work are as follows:

a) The sharp hike in the PoS attacks and complaince with regulations lead to the huge increase in market size of PoS security, which is estimated to grow from USD 4.0 Billion in 2022 to USD 6.1 Billion by 2027, but the existing PoS security solutions are hindering the market growth [1].
b) According to [2], the cybersecurity market will reach $300 billion by 2027 globally mainly in the realms of network security & privacy, cloud computing and in the telecommunication industry. The most recent DDoS attacks on the Abu Dhabi Commercial Bank and the National Bank of Fujairah brought down their websites [3].

Payment solutions help in making payments anywhere and at any time. Mobile Payment Applications (MPAs) and PoS Payment Applications (PPAs) are very important in the successful implementation of online commerce solutions. The authentication process of PoS based payments are performed in a public channel which are vulnerable to all types of attacks. In order to overcome any type of attack we need to design a secure and robust

Manuscript received June 5, 2024
Manuscript revised June 20, 2024
https://doi.org/10.22937/IJCSNS.2024.24.6.6

payment framework which embeds security from the design phase.

Limitations in the existing literature: Existing PoS based mobile payments has the following limitations

a) Payment Application's integrity in the smart phone and PoS are compromised.
b) Payment Applications in the smart phone and PoS are vulnerable to reverse engineering attacks
c) Smart phone, PoS and Bank Server's integrity is compromised in the existing PoS based mobile payment frameworks.
d) Existing PoS based mobile payment frameworks do not perform *point-to-point encryption which is very important for merchant based transactions.*
e) PoS based mobile payment frameworks are vulnerable to Heartbleed vulnerability.
f) Communication security of the transaction is compromised
g) Communication and Computational cost of the PoS based mobile payment frameworks are very high

Contributions made: Following are the contributions made by Smart and Secure PoS (SSPoS) Framework

a) In SSPoS Framework, Attackers fail to compromise the Payment Application's integrity in the smart phone and PoS as these applications are obfuscated

b) This paper proposes an architecture and procedure to provide security of the Application code, Security and Safety of the keys, Security of data in memory, Security of data at rest, end to end and Security of data during the transit.
c) In SSPoS Framework, Payment Applications in the smart phone and PoS are not vulnerable to reverse engineering attacks as these applications are obfuscated
d) In SSPoS Framework, Attackers fail to compromise the integrity of Smart phone, PoS and Bank Server in our framework as we make use of Secure Element and Trusted Platform Module (TPM).
e) SSPoS Framework performs *point-to-point encryption using AES encryption algorithm.*
f) SSPoS Framework withstands or overcomes Heartbleed vulnerability using TLS protocol
g) Communication and Computational cost of the SSPoS Framework is very less.
h) Proposed SSPoS framework adheres to the PCIDSS standard.

This article is organized as follows: Section II presents the related work. Section III presents proposed SSPoS framework. Section IV presents BAN logic based formal verification, Section V presents Threat Modeling, Section VI presents an experimental result, and section VII compares SSPoS with the related works. Section VIII provides discussion of SSPoS framework, and Section IX concludes the paper.

II. RELATED WORK

Following are the limitations of [2]

I. This work claims that it ensures only authentication but for a secure transaction all the security properties need to be ensured which includes mutual authentication, non-repudiation, integrity and confidentiality.
II. This work hasn't addressed POS (Point of Sale) vulnerabilities which are very crucial for the end to end security of the transaction.
III. There is no clarity how and from where the evidence is extracted from the client's device and merchant's machines in order to resolve disputes.

The research wok proposed by the Authors of [4] fails in ensuring non-repudiation property and moreover the key management is not effective. The research wok proposed by the Authors of [5] fails to address POS (Point of Sale) vulnerabilities which are very crucial for the end to end security of the transaction. In addition to this, authors of [5] work failed ensure optimal key management. The research wok proposed by the Authors of [6] has the following drawbacks

I. There is no clarity how and from where the evidence is extracted from the client's device and merchant's machines in order to resolve disputes.
II. Non-Repudiation property is not ensured
III. Key management is not effective

The research wok proposed by the Authors of [7] has the following limitations

I. This work claims that it ensures only authentication but for a secure transaction all the security properties need to be ensured which includes mutual authentication, non-repudiation, integrity and confidentiality.
II. This work hasn't addressed POS (Point of Sale) vulnerabilities which are very crucial for the end to end security of the transaction.
III. There is no clarity how and from where the evidence is extracted from the client's device and merchant's machines in order to resolve disputes.

III. PROPOSED SSPoS FRAMEWORK

NOTATION	FULL FORM	NOTATION	FULL FORM	NOTATION	FULL FORM
PCIDSS	Payment Card Industry Data Security Standard	**TEE**	Trusted Execution Environment	**OI**	Order Information
PoS	Point of Sale	**TSM**	Trusted Service Manager	$\mathbf{H(OI)}$	Hashed Order Information
SE	Secure Element	**CA**	Certifying Authority	$\mathbf{SK_{CB}}$	Shared Symmetric key between 'C' & 'B'
UICC	Universal Integrated Circuit Card	**TL**	Trust Levels	$\mathbf{T_{C}}$	Time Stamp of Customer
MPA	Mobile Payment Application	**M**	Merchant	$\mathbf{N_{C}}$	Nonce of
PPA	PoS Payment Application	**C**	Customer	$\mathbf{SK_{MB}}$	Shared Symmetric key between 'M' & 'B'
ECDSA	Elliptic Curve Digital Signature Algorithm	**SSPoS**	Smart and Secure Point of Sale	$\mathbf{N_{M}}$	Nonce of Merchant
AES	Advanced Encryption Standard	**P2PE**	*Point-to-Point Encryption*	$\mathbf{T_{M}}$	Time Stamp of Merchant
NFC	Near-Field Communication	**NFC**	Near Field Communication	$\mathbf{LOC_{C}}$	Location of Customer
PI	Payment Information	$\mathbf{(PI)SK_{CB}}$	Payment Information encrypted using Symmetric key shared between 'C' & 'B'	$\mathbf{LOC_{M}}$	Location of Merchant
AMT	AMOUNT	TransID	Transaction Identity		

Table 1:NOTATIONS

Customer (C), Merchant (M) and Bank (B) are the players in Secure PoS (SSPoS) Framework. Merchant (M) contains POS machine and NFC-enabled POI Device. POS Machine contains Secure Element, POS Application, Application Memory, Payment Client Application and Data Storage. Customer's NFC-enabled Smart Phone contains SE. The bank has Trusted execution environment (TEE) which is trusted and Applications are isolated and the Keys cannot be compromised. Following are the four locations in which SSPoS framework keeps the data secure

a) Data in Memory: When the payment application processes an authorization or settlement, it performs various manipulations with the payment card data in the memory of the hosting computer (usually the RAM of the POS machine).

b) Data at Rest: MPA and PPA keeps transaction data secure either temporarily or permanaently on the hard drive of Bannk and Merchant.

c) Data in Transit: Whenever the transaction data is in transit, the data should not be compromised.

d) Integrity of the Application:The integrity of both MPA and PPA should not be compromised i.e. these applications needs to with stand reverese engineering attacks from intruders. .

SSPoS framework uses point-to-point encryption (P2PE), as this method ensures encryption on the device and then allows the encrypted data for transmission to be processed by the third-parties for processing. *SSPoS framework hardens the MPA and PPA applications by obfuscating, by digitally signing, updating and patching these applications (MPA and PPA). In addition to these safety measures to the MPA and PPA applications, SSPoS framework adds* dynamic library to these applications, this method is called application wrapping.

Proposed Protocol

Step 1: Customer (C) selects items from the super market and reaches the Merchant (M). 'M' contains 'PoS', which interacts with the 'C'. 'C' uses his mobile payment application and sends

the following message to the 'PoS'

Step 1: $\mathrm{C} \rightarrow \mathrm{M}: \{\mathrm{MS1}\}$

Step 1: $\mathrm{C} \rightarrow \mathrm{M}: \{\mathrm{T_C}, \mathrm{N_C}, \mathrm{ID_C}, \mathrm{ID_M}, \mathrm{H(OI)}, \mathrm{OI}, \mathrm{(PI)SK_{CB}}, \mathrm{LOC_C}\}$

Step 2: Merchant (M) sends 'MS2' to the Bank (B) after successfully verifying the received 'MS1' from the Customer (C).

Step 2: $\mathrm{M} \rightarrow \mathrm{B}: \{\mathrm{MS2}\}\mathrm{SK_{MB}}$

Step 2: $\mathrm{M} \rightarrow \mathrm{B}: \{\mathrm{T_C}, \mathrm{N_C}, \mathrm{ID_C}, \mathrm{ID_M}, \mathrm{H(OI)}, \mathrm{OI}, \mathrm{(PI)SK_{CB}}, \mathrm{LOC_C}, \mathrm{LOC_M}, \mathrm{T_M}, \mathrm{N_M}\}\mathrm{SK_{MB}}$

Step 3: Bank verifies the received message 'MS2' from the merchant 'M', if the verification is successful then it transfers the funds to the M's account and updates about the transaction to both the merchant 'M' and customer 'C'

Step 3: **B**→M & C: $\{\mathrm{MS3}\}\mathrm{SK}_{\mathrm{PH}}$

MS3= {TransID, AMT}

IV. 'BAN LOGIC' BASED FORMAL VERIFICATION

BAN logic [8-10] classifies objects as principals, cryptographic keys and statements. These are represented symbolically as K_{cb} and K_{mb} are the shared symmetric keys in the proposed framework.

Step 1: C→ M: $\{T_C, N_C, ID_C, ID_M, H(OI), OI, (PI)SK_{CB}, LOC_C\}$

Step 1: 'M' verifies the received 'MS1' message from 'C'

M believes $\{\mathbf{T_C, N_C, ID_C, ID_M, H(OI), OI, (PI)SK_{CB}, LOC_C}\}$ --- (1)

M **believes C said** {MS1}-- (2)

So, from the statements (1) to (2)

M **believes** {MS1}-- (3)

Step 2: Bank 'B' receives $\{\mathrm{MS2}\}\mathrm{SK}_{\mathrm{MB}}$ and decrypts the message received from 'M',

B **believes M said:** $\{\mathrm{MS2}\}\mathrm{SK}_{\mathrm{MB}} - -(4)$

B **believes # $\mathbf{N_C}$ ----**(5)

B **believes # $\mathbf{N_M}$** --(6)

B **believes # $\mathbf{T_C}$** ---(7)

B **believes # $\mathbf{T_M}$** --(8)

B **believes # LOC**--(9)

From the statements (1) to (9) messages communicated among the entities are secure.

V. THREAT MODELING

In SSPoS framework threat modeling is classified in three steps

(1) **Assets and access points identification and the trust levels:** An asset is a valuable thing owned by a player of SSPOS framework, and the adversaries wants to manipulate it. Access points are the interfaces through which the adversaries try to can interact with the system in order to gain access to assets. Intruders use access points to enter into the system. There are different levels of trust defined by boundaries.

List of Assets in our proposed SSPOS framework: Mobile Payment Application (MPA), Smart Phone, Point of Sale (PoS), PoS Payment Application (PPA), TEE (Trusted Execution Environment) in the merchant side.

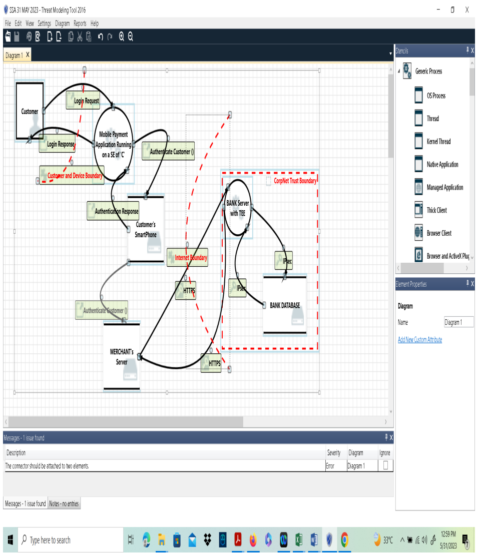
List of Access Points (AP) in our proposed SSPOS framework: Mobile Payment Application (MPA), Smart Phone, Point of Sale (PoS), PoS Payment Application (PPA).

Trust Levels (TL) in SSPoS framework: There are 3 trust boundaries in SSPoS framework.

i) **Customer and Device boundary:** Customer and Smart phone boundary is between Customer and the MPA in the SE (Secure Element) of the smartphone.

ii) **NFC (Near Field Communication) boundary:** NFC boundary is between Customer's smartphone and the M's PoS, Customer encrypts the messages using the shared symmetric key between 'C' and 'B' ensuring application security.

iii) **CorpNet Trust boundary:** CorpNet Trust boundary is between the Merchant (M) and the M's database and Bank (B) and its database, messages are protected using TLS protocol.



Description	Severity	Diagram	Ignore
The connector should be attached to two elements.	Error	Diagram 1	□

Fig. 1. Threat Modeling of SSPoS farmework

(2) **Recognize and Rank all the possible threats**: Threats are recognized by examining the assets and access points in the SSPoS framework which compromise the security properties such as authentication, confidentiality, non-repudiation, availability and integrity.

(3) **Discover solutions and make mitigation plan:** After recognizing the assets and threats there should be solutions to overcome these threats.

a) **Solutions for Spoofing:** Spoofing is not possible in SSPOS framework as all the entities store their credentials in the SE and TEE.

b) **Solutions for Tampering:** Tampering is not possible in SSPOS framework as all the entities exchange only encrypted messages among themselves.

c) **Solutions for Repudiation:** SSPOS employs Auditing Manager (AM), which works in coordination with CA.

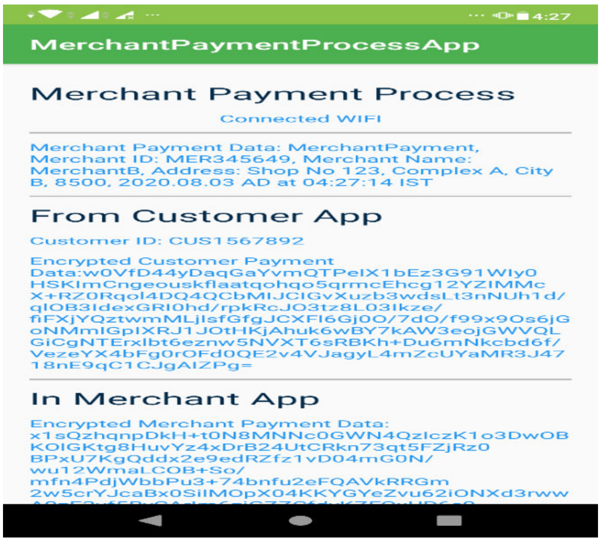
d) **Solutions for Information Disclosure:** Information disclosure is not possible in SSPOS framework as all the entities exchange only encrypted messages among themselves which ensures confidentiality.

e) Solutions for Denial of service: SSPOS framework uses “Fortguard Anti-DDoS” tool in order to overcome Denial of Service attacks.

f) **Solutions for Elevation of privilege:** End to end security which involves application and communication security will be able to overcome attacks in order to elevate the privileges.

VI. EXPERIMENTAL SETUP AND RESULTS

SSPOS is implemented in Android Studio using Kotlin language.



MerchantPaymentProcessApp

Merchant Payment Process

Connected WIFI

Merchant Payment Data: MerchantPayment, Merchant ID: MER345649, Merchant Name: MerchantB, Address: Shop No 123, Complex A, City B, 8500, 2020.08.03 AD at 04:27:14 IST

From Customer App

Customer ID: CUS1567892

Encrypted Customer Payment Data:w0VfD44yDaqGaYvmQTPelX1bEz3G91WIy0HSKImCngeouskflaatqohqo5qrmcEhcg12YZIMMcX+RZ0Rqol4DQ4QCbMIJCIGvXuzb3wdsLt3nNUh1d/qIOB3IdexGRI0hd/rpkRcJO3tz8L03Ikze/fiFXjYQztwmMLjIsfGfgJCXFI6Gj0O/7dO/f99x9Os6jGoNMmIGpIXRJ1JOtHKjAhuk6wBY7kAW3eojGWVQLGiCgNTErxlbt6eznw5NVXT6sRBKh+Du6mNkcbd6f/VezeYX4bFg0rOFd0QE2v4VJagyL4mZcUYaMR3J4718nE9qC1CJgAIZPg=

In Merchant App

Encrypted Merchant Payment Data: x1sQzhqnpDkH+t0N8MNNc0GWN4QzlczK1o3DwOBKOIGKtg8HuvYz4xDrB24UtCRkn73qt5FZjRz0BPxU7KgQddx2e9edRZfz1vD04mG0N/wu12WmaLCOB+So/mfn4PdjWbbPu3+74bnfu2eFQAVkRRGm2w5crYJcaBx0SiIMOpX04KKYGYeZvu62iONXd3rww

Fig. 2. Experimental Results of SSPoS framework

VII. COMPARISON WITH RELATED WORK

This section presents the comparative analysis of our proposed SSPoS framework. Table compares SSPoS framework with the related works discussed in the section 2. SSPoS framework has the best features than the features discussed in related works.

Research Works Features	[4]	[5]	[6]	[7]	Our Proposed
Confidentiality	No	No	No	Yes	Yes
Authentication				Yes	Yes
Integrity	No	No	No	Yes	Yes
PCIDSS standard	No	No	No	No	Yes
Ensures Application Security	No	No	No	No	Yes
Ensures Communication Security	No	No	No	Yes	Yes
Withstands Heartbleed Vulnerability	No	No	No	Yes	Yes
Withstands Replay Attacks	No	No	No	No	Yes
Withstands Man-In-The-Middle Attacks	No	No	No	No	Yes
Withstands Impersonation Attacks	No	No	No	No	Yes
Withstands reverse engineering attacks	No	No	No	No	Yes

Table 2: Comparision with related works

VIII. PERFORMACE ANALYSIS

We compared the performance analysis of our proposed SSPoS framework with the related work in terms of "overall energy cost in Micro Joules" and "overall computational cost in Seconds". According to [11], the time complexities calculated in seconds are TH = 0.0004 seconds and TS = 0.1303 seconds. As per [12] One ECPM (Elliptic Curve Point Multiplication) is 0.001015 seconds. SSPoS framework has better performance compared with the related works. As per [5] the energy required to generate AES encryption/decryption (ES) is 1.21 Micro Joules/byte and for generating hash code (EH) using SHA-1 algorithm is 0.76 Micro Joules. As per [12] the energy required for One ECPM (Elliptic Curve Point Multiplication) is equal to 578.55 Micro Joules from [12].

Protocol	Overall computation cost in seconds
[4]	8TS+6TSig+8TH (1.05169)
[6]	7TS+2TSig+2TH (0.91493)
[7]	12TS+22TH (1.5724)
Our Proposed	2 TS+2TH (0.2614)

Table 3: Overall energy cost of SSPoS protocol

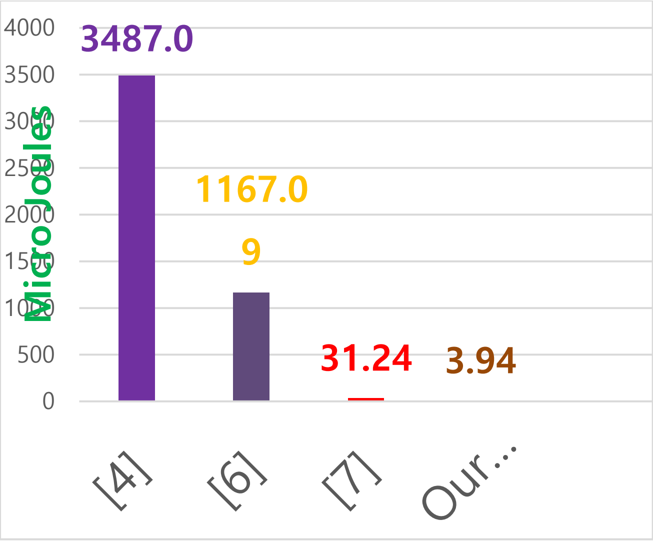


Fig. 3. Bar Chart for overall energy cost of SSPoS protocol

Protocol	Overall Energy cost in Micro Joules
[4]	8ES+6ESig+8EH 8(1.21) +6(578.55) +8(0.76) =3487.06
[6]	7ES+2ESig+2EH 7(1.21) +2(578.55) +2(0.76) =1167.09
[7]	12ES+22EH 12(1.21) +22(0.76) =31.24
Our Proposed	2 ES+2EH 2(1.21) +2(0.76) =3.94

Table 4: Overall Computational Cost of SSPoS protocol

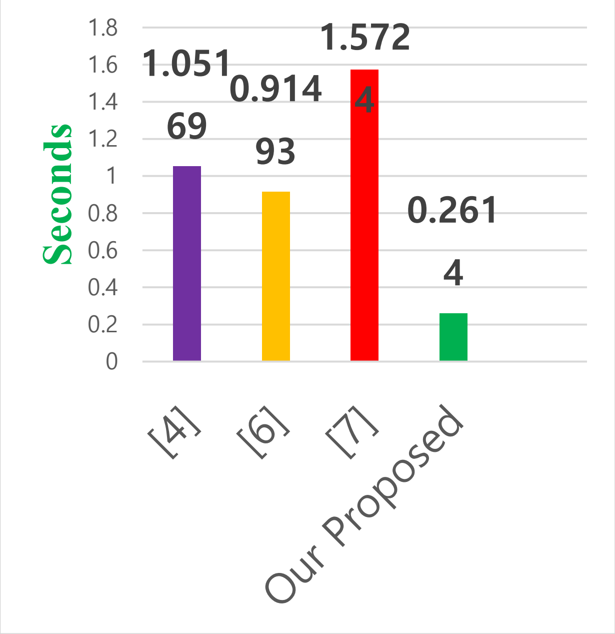


Fig. 4. Bar Chart for Overall Computational Cost of SSPoS protocol

IX. DISCUSSION

Payments industry is the main target of intruders especially PoS based payments. Intruders exploit four attack surfaces, they are User Credentials, Application Integrity, Device Integrity (Smart phone, PoS and Bank Server) and communication security. Following are the recommendations for PoS based payments solutions.

a) PoS based payment solutions should ensure end to end security.
b) PoS based payment solutions should be in compliance to PCIDSS standard.
c) PoS based payment solutions should overcome reverse engineering attacks
d) PoS based payment solutions should overcome heart-bleed vulnerabilities.
e) PoS based payment solutions should overcome DoS and DDoS attacks.
f) PoS based payment solutions should adopt SE, TPM and TEE in order to withstand most of the attacks.

X. DISCUSSION

Payments industry is the main target of intruders especially PoS based payments. Intruders exploit four a Server) and communication security. Following are the recommendations for PoS based payments solutions

g) PoS based payment solutions should ensure end to end security.
h) PoS based payment solutions should be in compliance to PCIDSS standard.
i) PoS based payment solutions should overcome reverse engineering attacks
j) PoS based payment solutions should overcome heart-bleed vulnerabilities.
k) PoS based payment solutions should overcome DoS and DDoS attacks.
l) PoS based payment solutions should adopt SE, TPM and TEE in order to withstand most of the attacks.

References

[1] https://www.globenewswire.com/news-release/2022/09/21/2519914/0/en/The-global-POS-Security-market-size-is-expected-to-grow-from-an-estimated-value-of-USD-4-0-billion-in-2022-to-USD-6-1-billion-by-2027-at-a-Compound-Annual-Growth-Rate-CAGR-of-8-6.html

[2] https://www.businesswire.com/news/home/20230123005388/en/Cybersecurity-Market---Global-Forecast-to-2027-Opportunities-Emerging-in-Increasing-Use-of-AI-ML-And-Blockchain-Technologies-for-Cyber-Defense---ResearchAndMarkets.com

[3] https://thecyberexpress-com.cdn.ampproject.org/c/s/thecyberexpress.com/cyber-attack-on-uae-banking-sector-adcb-nbf/amp/

[4] Lu H-J, Liu D (2021) An improved NFC device authentication protocol. PLoS ONE 16(8): e0256367. https://doi.org/10.1371/journal.pone.0256367

[5] Brij B. Gupta and Shaifali Narayan, “A Key-Based Mutual Authentication Framework for Mobile Contactless Payment System Using Authentication Server”. Journal of Organizational and End User Computing, Volume 33(2), March-April 2021

[6] Forough Sadat Mirkarimzade Tafti, Shahriar Mohammadi, Mehdi Babagoli, “A new NFC mobile payment protocol using improved GSM based authentication,” *Journal of Information Security and Applications*, vol. 62, pp. 1–10, Nov. 2021

[7] M. Alshammari and S. Nashwan, "Fully authentication services scheme for nfc mobile payment systems," *Intelligent Automation & Soft Computing*, vol. 32, no.1, pp. 401–428, 2022.

[8] S. Muhammad, Z. Furqan, and R. K. Guha, "Understanding the intruder through attacks on cryptographic protocols," in *Proc. Annual Southeast Conference*, Melbourne, Florida, USA, vol. 2006, pp. 667–672.

[9] M. Abadi, M. Burrows, C. Kaufman, and B. Lampson, "Authentication and delegation with smart-cards," *Sci. Comput. Program.*, vol. 21, no. 2, pp. 93–113, Oct. 1993.

[10] M. Burrows, M. Abadi, and R. Needham, "A logic of Authentication," *ACM Trans. Comput. Syst.*, vol. 8, no. 1, pp. 18–36, Jan. 1990.

[11] [5] J.-H. Yang, Y.-F. Chang, and Y.-H. Chen, ‘‘An efficient authenticated encryption scheme based on ECC and its application for electronic pay-ment,’’ Inf. Technol. Control, vol. 42, no. 4, pp. 315–324, Dec. 2013.

[12] M. H. Ibrahim, S. Kumari, A. K. Das, and V. Odelu, ‘‘Jamming resis-tant non-interactive anonymous and unlinkable authentication scheme for mobile satellite networks,’’ Secur. Commun. Netw., vol. 9, no. 18, pp. 5563–5580, Dec. 2016.