CHAPTER ONE

1.0 INTRODUCTION

1.1 Background

The world has changed with the advent of internet and its use has created a revolution in almost all spheres of life. There is a high dependency upon web based services for even transactions and nobody is complaining as it offers a world of convenience to the payment process.

E-commerce has been transformed by the emergence of the electronic payment system (EPS), which is rapidly shaping the way business is conducted in the digital world. (Summers, 2012), e-commerce is a payment mode for buying and selling of goods and services offered through the internet. According to (Harris, Guru, B.K, & Avvari, M.V, 2011), most e-commerce transactions involve the buying and selling of goods and services and payment for these goods and services. Because traditional payment methods cannot be effectively used to complete an electronic transaction, EPS has emerged as an attractive alternative because of its features such as security, simplicity, convenience, reliability, privacy, and anonymity.

The adoption process of EPS has though been a silent revolution because these extensive changes have occurred slowly and not necessarily in ways that are obvious. The traditional, trusted and convenient means of effecting payments still have a strong attraction to consumers, who therefore change their economic behavior slowly because of their emotional relationship to money and the payment mechanisms they trust. (Vartanian, Ledig, R.H., & Ansell, D.L, 2004).

Although this has been the case the adoption proceedings have been impressive but not satisfactory as there have been a few issues when it comes to entrusting ones financial

and personal information that is needed for the implementation of these systems without having doubts of its breach or misuse in the future.

This created a forum that geared a research to look into the aspect of security determining the effects of security in regards to adoption of EPS systems. It gave an overview of what forms of security issues are in EPS systems.

The focus was on spoofing attacks and what forms of solutions have been captured to help curb this issue and in particular it focused on an integration of Stack PI and Encryption as the main methodologies.

1.2 Statement of the Problem

The issue of security bears an enormous role when it comes to adoption and performance of EPS systems, regardless of how beneficial, affordable and fast when it comes to service provision there is still rigidness in their implementation. The three most significant areas plaguing successful implementation of EPS globally are trust, security, and privacy (Sumanjeet, 2009). According to CERT, the number of reported Internet security incidents has jumped from 6 in 1988 to 82,094 in 2002, and the number of Internet security incidents in 2003 was 137,529 (CERT, 2006).

(Messmer, 2007) edition features an article on the costs of data breaches, a study conducted by the Ponemon Institute. The Ponemon study found that it costs an average of $182 for each compromised data record, which is up from $138 from the previous year, an increase of over 30%. There have now been roughly 100 million notifications sent to individuals in the US notifying them that their personal information has been compromised (Moyle, 2007). Several reasons contribute to this insecurity examples of these include; spoofing attacks, eavesdropping, acting under false identity, exploits, social engineering, human error, denial of service attacks, indirect attacks and also backdoors among others. Stealing data is undetectable in most of these cases.

Among these insecurities the focus was on spoofing attacks as it influences EPS systems the most, to narrow it down emphasis was placed on IP spoofing as the most infamous form of spoofing attack on these systems. In this case, attackers often spoof the source IP address of their packets and thus evade traditional packet filters. Unfortunately, the current routing infrastructure cannot detect that a packet's source IP address has been spoofed or from where in the Internet a spoofed IP packet has originated from. The combination of these two factors makes IP spoofing easy and effective for attacks. In fact, many different types of Internet attacks utilize spoofed IP addresses for different purposes, (Gupta & Kavyashree, H, 2013).

1.3 Justification

The main reason for participating in this research is to contribute to the security solutions of EPS system by giving a viable solution on how to deal with spoofing attacks. The integration of the already existing working standalone solutions is bound to provide a better security platform in comparison to their standalone counterparts as they are destined to complement each other's weaknesses and strengths.

This research would contribute highly to the reduction of cost incurred to prevent spoofing attacks and enable the full abilities that electronic payment systems are willing to offer this generation of business to be appreciated. EPS abilities set at 100 percent would mean enormous savings as these systems are more effective and efficient in comparison to their traditional payment systems counterparts. This led to embarking on this research and try to bridge an evident gap on defense against spoofing attacks on EPS systems.

1.4 Research Objectives

1.4.1 General Objective

To examine the effects of spoofing attacks on the adoption of online EPS systems.

1.4.2 Specific Objectives

i. To determine the awareness level of spoofing attacks on online payment systems.
ii. To examine some of the techniques that have been developed and applied to curb the presence of spoofing attacks.
iii. To determine if a combination of this techniques performs better in comparison to the standalone techniques.
iv. To evaluate the efficacy of the combination of Stack Pi and Encryption informed by machine learning.

1.4.3 Research Questions

i. Do consumers realize the existence of spoofing attacks on online payment systems?
ii. What techniques have been adopted to curb the presence of spoofing attacks?
iii. What techniques have been combined to prevent spoofing attacks?
iv. What efficiency levels does a combination of Stack Pi and Encryption informed by machine learning have on the prevention of spoofing attacks?

1.5 Scope of Study

This study focused on online payments via financial institutions websites as one of the electronic payment gateways which reviewed how spoofing attack actually affects its wide usage, acceptance and implementation. Since IP spoofing is the most common form of spoofing attack this study will predominantly focus and use it for illustration, the defense strategies however are largely similar for all spoofing attacks.

1.6 Limitations of the Study

Company policy restrictions were main obstacles to collecting the data.

Lack of cooperation from financial institutions as admission of this was a liability as it meant admission of having a security issue in their system. Spoofing attacks in financial institutions could be detrimental especially if this knowledge is leaked to the market it can lead to loss of customers as they might feel vulnerable with their information.

1.7 Definition of Terms

Authentication- The assurance that the communicating entity is the one that it claims to be.

BGP routing - is a protocol for exchanging routing information between gateway hosts (each with its own router) in a network of autonomous systems on the internet.

Classless Inter -Domain Routing - an IP addressing scheme that replaces the older system based on classes A, B, and C. A single IP address can be used to designate many unique IP addresses with CIDR. A CIDR IP address looks like a normal IP address except that it ends with a slash followed by a number, called the IP network prefix.

Distributed packet filtering - packet filtering is the process of passing or blocking packets at a network interface based on source and destination addresses, ports, or protocols.

Distributed Denial of Service - is a type of DOS attack where multiple compromised systems which are usually infected with a Trojan are used to target a single system causing a Denial of Service (DoS).

Drop - Using the DROP rule instructs the firewall to be more silent in its denial. Packets that arrive are dropped without sending an ICMP port unreachable back to the initiator.

The connection will be rejected, but the initiator will simply assume that no service is running on the target host (or that the target host does not exist).

Electronic Payment System - is a financial exchange that takes place online between buyers and sellers by some form of digital financial instrument.. The content of this exchange is usually some form of digital financial instrument that is backed by a bank or an intermediary.

E-commerce - is the buying and selling of goods and services on the Internet, especially the World Wide Web. In practice, this term and a newer term, e-business, are often used interchangeably.

Time To Live - is a value in IP packet that tells the network router whether or not the packet has been in the network for too long and should be discarded.

Secure Socket Layer is a commonly-used protocol for managing the security of a message transmission on the Internet. SSL has recently been succeeded by Transport Layer Security (TLS), which is based on SSL. SSL uses a program layer located between the Internet's Hypertext

Spoofing attack - is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.

Network Ingress Filtering- is a technique used to make sure that incoming packets are actually from the networks that they claim to be from.

Ingress filtering - is a technique used to make sure that incoming packets are actually from the networks that they claim to be from.

ICMP message - is one of the main protocols of Internet Protocol Suite. It is used by network devices like routers to send error messages indicating for example that a requested service is not available.

IP Spoofing - The attacker can create IP packets by modifying the selected fields that contain addresses or identifiers with values that belong to others. During an attack, the attacker generally desires to be anonymous but, the system administrators can monitor the packets the host is receiving and can get the details of the source location. Hence, IP spoofing is frequently used by the attackers to impersonate others and to maintain anonymity.

Router - Routers are the Internet devices used to forward the data packets from one entity to another. The entity can either be a host or a server or any other router. Routers use the information present in the packet headers to determine the best path for forwarding the packets.

Spoofing Attack - it is well-known attack technique in both wired and wireless networks. The attacker can gain access to the network and its resources by constructing frames and filling fields containing addresses or identifiers with forged values that belong to others. These addresses or identifiers may be IP addresses or MAC addresses that are unique for each host in the network. Spoofing attack can be classified according to the identifier that the attacker had spoofed.

CHAPTER TWO

2.0 LITERATURE REVIEW

2.1 Introduction

This chapter presented the review of literature focused on the effects of security on adoption of electronic payment systems by focusing on spoofing attacks as one of the key security issue. The focus was on the supply side of electronic payment system where reviews on what the already existing techniques implemented to curb spoofing attacks had accomplished and the gaps that still existed. An assessment on integrated solutions previously applied and their success rates was reviewed and a justification on why the integration of Stack Pi, Encryption and Machine Learning would be a success was reached.

2.2 Spoofing Attacks

Spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage in a spoofing attack, the attacker creates misleading context in order to trick the victim into making an inappropriate security-relevant decision, (Upadhyay & Kumar, R., 2011).

Sending IP packets with fake source addresses is known as packet spoofing and is used by attackers for numerous purposes. These include obscuring the correct source of the attack, implicating an additional site as the attack source, pretending to be a trusted host, hijacking or interrupting network traffic, or causing replies to goal another system, (Linta, S & Khan, R, 2013).

One of the most difficult challenges in defending against spoofing is that attackers often spoof the source IP address of their packets and thus evade traditional packet filters. Unfortunately, the current routing infrastructure cannot detect that a packet's source IP address has been spoofed or from where in the Internet a spoofed IP packet has

originated from, (Gupta & Kavyashree, H, 2013). The combination of these two factors makes IP spoofing easy and effective for attacks. In fact, many different types of Internet attacks utilize spoofed IP addresses for different purposes.

In today's Internet, (Linta, S & Khan, R, 2013) noted that attackers can forge the source address of IP packets to both maintain their anonymity and redirect the blame for attacks. When attackers inject packets with spoofed source addresses into the Internet, routers forward those packets to their destination just like any other packet often without checking the validity of the packet's source addresses.

IP Spoofing is one of the major tools used by hackers in the internet to mount spoofing attacks. In such attacks the attackers duplicate the Source IP of packets that are used in the attack. Instead of carrying the original source IP of the machine the packet came from, it contains an arbitrary IP address which is selected either random fashion or particularly. The ease with which such attacks are generated made them very popular (Wyld, Wozniak, Chaki, Meghanathan, & Nagamalai., 2011).

To be successful, the intruder must first find out the IP address of a trusted system, and then change the packet headers such that it appears that the packets are impending from the trusted system. In IP address spoofing Internet Protocol packets are created with forged source IP address. The main aim of spoofing is for hiding sender identity. In this the attacker without authority access computer or network showing as if malicious message came from trusted machine by spoofing that machine Address, (Gupta & Kavyashree, H, 2013).

2.3 Customer perspective on web security

It is considered that 64 percent of online consumers are unlikely to trust a Web site, even if the site prominently features a privacy policy (Pastore, 2000). In conjunction with these studies, a number of key factors influencing perception of e-payment are proposed. (Hataiseree & Banchuen, W, 2010) found that cash and cheques remain as popular

payment modes because consumers are not convinced of the benefits of using e-payment. (Abrazhevich, 2001) attributes e-payment's failure to the system design and deployment that do not meet user requirements and expectations.

These studies suggest that security, trust, benefits, self-efficacy, and ease of use are important factors influencing perception of e-payment. Very few studies to date have attempted to study these factors in a single setting ((Haque, Tarofder, A.K, Rahman, S., & Raquib, M.A, 2009). Because of this, many researchers maintain that trust is essential for understanding interpersonal behavior and economic exchanges which affects customers' perception toward e-payment systems (Abrazhevich, 2001) and subsequently its adoption success (Chau & Poon, 2003; Kniberg, 2002; Lim, Lee, H., & Kurnia, S. , 2006).

That is the reason why (Kniberg, 2002) insists that trust is more important than security. In fact Kniberg opines that users and merchants are more likely to use an insecure payment system from a trusted company than a secure payment system from an untrusted company. It can therefore be concluded that trustworthiness is vital to e-payment success (Abrazhevich, 2001).Without an adequate system that users can trust, it would be extremely difficult for e-payment to achieve widespread usage (Lim, Lee, H., & Kurnia, S. , 2006).

2.4 Customer knowledge on Spoofing Attacks

In a spoofing attack, the attacker creates misleading context in order to trick the victim into making an inappropriate security-relevant decision. A spoofing attack is like a con game: the attacker sets up a false but convincing world around the victim. The victim does something that would be appropriate if the false world were real. Unfortunately, activities that seem reasonable in the false world may have disastrous effects in the real world, (Felten E. , Balfanz, D., Dean, D., & Wallach, D.S, 1997).

People using computer systems often make security-relevant decisions based on contextual cues they see. For example, one might decide to type in their bank account number because they believe they are visiting their bank's Web page. This belief might arise because the page has a familiar look, because the bank's URL appears in the browser's location line, or for some other reason. The appearance of an object might convey a certain impression; for example, neon green text on a purple background probably came from wired magazine. You might think you're dealing with a popup window when what you are seeing is really just a rectangle with a border and a color different from the surrounding parts of the screen. Particular graphical items like file-open dialog boxes are immediately recognized as having a certain purpose. (Felten E. , Balfanz, D., Dean, D., & Wallach, D.S., 2013).

If two things happen at the same time, one naturally thinks they are related. If one clicks over to your bank's page and a username/password dialog box appears, one naturally assumes that they should type the name and password that they use for the bank. If one is to click on a link and a document immediately starts downloading, one assumes that the document came from the site whose link they clicked on. Either assumption could be wrong. If one only sees one browser window when an event occurs, they might not realize that the event was caused by another window hiding behind the visible one. Modern user-interface designers spend their time trying to devise contextual cues that will guide people to behave appropriately, even if they do not explicitly notice the cues. While this is usually beneficial, it can become dangerous when people are accustomed to relying on context that is not always correct. (Minsky, 2010).

2.5 Forms of Spoofing

The main aim of spoofing is for hiding sender identity. In this attacker unauthorizingly access computer or network showing as if malicious message came from trusted machine by spoofing that machine Address, (Gupta & Kavyashree, H, 2013). The most

common spoofing attacks are MAC address spoofing and IP address spoofing,(Bhaya & Alasady, 2012).

2.5.1 IP Spoofing

IP Spoofing is one of the major tools used by hackers in the internet to mount spoofing attacks. In such attacks the attackers duplicate the Source IP of packets that are used in the attack. Instead of carrying the original source IP of the machine the packet came from, it contains an arbitrary IP address which is selected either random fashion or particularly. The ease with which such attacks are generated made them very popular, (Wyld, Wozniak, Chaki, Meghanathan, & Nagamalai., 2011). To be successful, the intruder must first find out the IP address of a trusted system, and then change the packet headers such that it appears that the packets are impending from the trusted system. In IP address spoofing Internet Protocol packets are created with forged source IP address. The Main aim of spoofing is for hiding sender identity. In this attacker without authority accesses the computer or network showing as if malicious message came from trusted machine by spoofing that machine Address. (Gupta & Kavyashree, H, 2013).

2.5.2 TCP and DNS Spoofing

According to (Douglas, 2006), TCP spoofing is a spoofing attack that tricks the user's software into an inappropriate action by presenting misleading information to that software. Examples of such attacks include TCP spoofing, in which Internet packets are sent with forged return addresses, and DNS spoofing, in which the attacker forges information about which machine names correspond to which network addresses.

2.5.3 Web Spoofing

(Keizer, 2006), web spoofing is a kind of electronic con game in which the attacker creates a convincing but false copy of the entire World Wide Web. The false Web looks just like the real one: it has all the same pages and links. However, the attacker controls

the false Web, so that all network traffic between the victim's browser and the Web goes through the attacker.

Since the attacker can observe or modify any data going from the victim to Web servers, as well as controlling all return traffic from Web servers to the victim, the attacker has many possibilities. These include surveillance and tampering.

According to (Felten E. , Balfanz, D., Dean, D., & Wallach, D.S, 1997), in surveillance the attacker can passively watch the traffic, recording which pages the victim visits and the contents of those pages. When the victim fills out a form, the entered data is transmitted to a Web server, so the attacker can record that too, along with the response sent back by the server. Since most on-line commerce is done via forms, this means the attacker can observe any account numbers or passwords the victim enters. The attacker can carry out surveillance even if the victim has a "secure" connection (usually via Secure Sockets Layer) to the server, that is, even if the victim's browser shows the secure-connection icon (usually an image of a lock or a key). In tampering the attacker is also free to modify any of the data traveling in either direction between the victim and the Web. The attacker can modify form data submitted by the victim. For example, if the victim is ordering a product on-line, the attacker can change the product number, the quantity, or the ship-to address.

The attacker can also modify the data returned by a Web server, for example by inserting misleading or offensive material in order to trick the victim or to cause antagonism between the victim and the server.

2.6 Measures to Curb Spoofing Attacks

A meta-analysis of some methodologies that have been implemented in the defense against spoofing attacks was critical for comprehension of general nature of spoofing attacks and the efficiencies of the methodologies employed under the given circumstances.

(Ferguson & Senie, 1998) proposed to deploy network ingress filtering to limit spoofing of the source IP address. Although it could help by preventing a packet from leaving a border network without a source address from the border network attackers have countered by choosing legitimate border network addresses at random. Also, every ISP had to implement this scheme otherwise there would have been entry points to the internet. To add to that the additional router configuration that was required and processing overhead to perform the filtering made it a not so much sought after remedy.

(Savage, Wetherall, D., Karlin, A., & Anderson, T, 2000) introduced a new scheme for providing traceback data by having routers embed information randomly into packets. They proposed a scheme in which adjacent routers would randomly insert adjacent edge information into the ID field of packets. Their key insight was that traceback data could be spread across multiple packets because a large number of packets were expected. They also include a distance field which allows a victim to determine the distance that a particular edge is from the host. This prevents spoofing of edges from closer than the nearest attacker. The biggest disadvantage of this scheme is the combinatorial explosion, where the problem that the number of combinations that one has to examine grows exponentially, so fast that even the fastest computers will require an intolerable amount of time to examine them. The combinatorial explosion problem limits the ability of computers to solve large problems. This is because in most realistic problems of interest to us, the number of combinations is typically very large.

(Lee & Park, K., 2001) propose a router packet filtering (RPF) mechanism against IP address spoofing. RPF relies on Border Gateways Protocol (BGP) routing information to detect spoofed IP addresses. According to (Peng, Joshi, J., & Tipper, D., 2006), their approach was interesting, but required high levels of router participation.

According to (Rekhter & Li, T. , 1995), source addresses are included in BGP messages, this would significantly increase the size and processing time for BGP messages. The third potential limitation is that RPF relies on valid BGP messages to configure the filter.

If an attacker can hijack a BGP session and disseminate bogus BGP messages, then it is possible to mislead border routers to update filtering rules in favor of the attacker. Finally, the filtering rules in RPF have a very coarse granularity, i.e., at the AS level. The attacker can still spoof IP addresses based on the network topology.

(Li, Wang, J.M.M., Reiher, P., & Zhang, L. , 2002) proposed the Source Address Validity Enforcement (SAVE) protocol which enables routers to update the information of expected source IP addresses on each link and block any IP packet with an unexpected source IP address. SAVE protocol is geared to provide routers with information about the range of source IP addresses that should be expected at each interface. Similar to the existing routing protocols; SAVE constantly propagates messages containing valid source address information from the source location to all destinations. Hence, each router along the way is able to build an incoming table that associates each link of the router with a set of valid source address blocks.

(Morein, Stavrou, A., Cook, D.L., Keromytis, A.D., & Misra, V, 2003) proposed a graphic turing test a complementary approach to blocking attack traffic is to limit the rate at which sources can generate requests. If a target service is designed for use by a person, then it may be reasonable to filter all traffic that is generated by an automated source, e.g., an attack zombie. When an unfamiliar source uses a service for the first time, then it must first complete an admission challenge that requires human judgment, such as reading a character string that has been presented as an image (Morein, Stavrou, A., Cook, D.L., Keromytis, A.D., & Misra, V, 2003). This denies access to automated sources, which would be unable to complete the challenge. Such challenges can be reissued to a source if that source starts to generate a large number of requests, i.e., the person has been replaced by an automated source. A variant on this approach has been proposed for target services that are intended for use by automated sources, e.g., DNS servers. In this case, the admission challenge takes the form of a computational puzzle,

which is designed to be easy to set and verify, but hard to solve, e.g., a constraint satisfaction problem (Kandula, Katabi, D., Jacob, M., & Berger, A., 2005).

In this case, any additional requests from a source are blocked until the initial challenge has been solved. However, this form of puzzle-based challenge requires compatible client software at the source, which may limit the deployment of this approach. Similarly, admission challenges that require human judgment can create more work for legitimate users, and may not achieve user acceptance. Furthermore, both types of challenge still require some computational resources at the target, which can become a bottleneck during an attack.

SAVE is a protocol that enables the router to filter packets with spoofed source addresses using incoming tables. It shares the same idea with ingress filtering and RPF that the source address space on each link of the router is stable and foreseen. Any packet that violates the expected source address space will be regarded as forged and will be filtered. SAVE outperforms ingress filtering and RPF in that it overcomes the asymmetries of Internet routing by updating the incoming tables on each router periodically. The limitations of SAVE needs to change the routing protocol, which will take a long time to accomplish. Moreover, as SAVE filters the spoofed packets to protect other entities, it does not provide direct implementation incentives. If SAVE is not universally deployed, attackers can always spoof the IP addresses within networks that do not implement SAVE. Moreover, even if SAVE were universally deployed, attackers could still launch Distributed Denial of Service attacks using non-spoofed source addresses.

(Minho & Jun, X, 2002), proposed an altered IP traceback approach, where the victim tries to reconstruct the attack path but also attempts to estimate if a new packet lies on the attack path or not. Their scheme was probabilistic and each router either inserts an edge marking for the IP traceback scheme or a router marking identifying the router. Unfortunately, their approach required the victim to collect on the order of 105 attack

packets to reconstruct a path, and once the path is reconstructed, this scheme was likely have a high false positive rate as the routers close to the victim would all lie on some attack path and frequently mark legitimate packets which would then get rejected.

2.6.1 Encrytion

Encryption is one of the methodologies for curbing spoofing attack. According to (Bacard, 1995), Cryptography is related to computer security, the word cryptography was originally derived from the Greek words of *kryptos* and *graphos*. *Kryptos* is defined as secret whereas *graphos* is defined as writing. Cryptography involves two processes which are encryption (scramble) and decryption (unscramble). Cryptography is a process of converting plaintext into cipher text, and in contrast ciphers text into plaintext (Haney, 2006). Plaintext is a term that refers to an original text. There are certain mathematical formulae or rules that can be used for the encryption and decryption processes. These mathematical formulae or rules are known as cipher.

Cryptographic techniques provide the logical protection of electronic money systems by ensuring the confidentiality, authenticity and integrity of devices, data and communications used in transactions. There are a number of different cryptographic techniques that are used for different purposes in electronic money systems.

Encryption is a technique used to protect the confidentiality of data during transmission or while stored on a device. Encryption is particularly important for certain types of sensitive data used in security processes, such as cryptographic keys. Other information, such as payment amounts or card serial numbers, may not necessarily be transmitted or stored in encrypted form. Firstly, overall cryptography is a long process and it takes a long time to figure out the code to use, if one was to send the code to another person in the past it would take a while to get to that person.

Secondly, the widespread availability of unbreakable encryption coupled with anonymous services could lead to a situation where practically all communications are

immune from lawful interception (wiretaps) and documents from lawful search and seizure, and where all electronic transactions are beyond the reach of any government regulation or oversight. Thirdly, encryption also threatens national security by interfering with foreign intelligence operations. The United States, along with many other countries, imposes export controls on encryption technology to lessen this threat. To add to that, cryptography poses a threat to organizations and individuals too. With encryption, an employee of a company can sell proprietary electronic information to a competitor without the need to photocopy and handle physical documents.

Fourthly, electronic information can be bought and sold on "black networks" such as Black-Net with complete secrecy and anonymity a safe harbor for engaging in both corporate and government espionage. The keys that unlock a corporation's files may be lost, corrupted, or held hostage for ransom, thus rendering valuable information inaccessible. Lastly, the application of cryptographic schemes requires reliable key distribution, management, and maintenance mechanisms. It is not always desirable to apply these cryptographic methods because of its infrastructural, computational, and management overhead. Further, cryptographic methods are susceptible to node compromise, which is a serious concern as most wireless nodes are easily accessible, allowing their memory to be easily scanned.

2.6.2 Stack Pi

Stack Pi is another methodology for defense against spoofing attack, according to (Shyamaladevi & Wahidabanu, R.S.D., 2008), StackPi is an abbreviation Stack Path Identifier, and is where a packet traverses routers on the path towards its destination; the routers deterministically mark bits in the packet’s IP Identification field. The deterministic markings guarantee that packets traveling along the same path will have the same marking.

StackPi allows the victim and routers on the attack path to take a proactive role in defending against a DDoS attack by using the StackPi mark to filter out attack packets on a per packet basis. In addition, the victim can build statistics over time relating StackPi marks to IP addresses. Then if an attacker spoofs an IP address, it is likely that the StackPi mark in the spoofed packet will not match the StackPi mark corresponding to the legitimate IP address in the database, thus enabling the victim to tag packets.

(Minho & Jun, X, 2002), the filter simply checks any incoming packet's StackPi mark and compares its IP address to a list of hIP address, StackPi marki tuples to see if there is a match. Like the threshold filtering scheme, the StackPi-IP filter requires bootstrapping however, in this case, with packets bearing non-spoofed source IP addresses. Such a scenario is ideal for a server that has a static set of authorized users.

(Perrig, Song, D., & Yaar, A, 2002), the metric that best quantifies the performance of the StackPi-IP filter is the probability that a randomly selected attacker will be able to spoof an IP address that will be accepted by the victim. The only way for this to happen is for an attacker to spoof the IP address of an end-host that happens to have the same StackPi mark as the attacker itself. This is hardest for the attacker when the IP addresses of end-hosts in the topology are distributed uniformly over the possible StackPi marks, because no StackPi mark has a large number of IP addresses that map to it and thus there are fewer IP addresses for that StackPi mark that will be accepted by the filter.

Machine Learning

There are various definitions of machine learning which is a subfield of computer science (CS) and artificial intelligence (AI) that deals with the construction and study of systems can learn from data, allowing them to handle new situations via analysis, self-training, observation and experience. Machine learning facilitates the continuous advancement of computing through exposure to new scenarios, testing and adaptation,

while employing pattern and trend detection for improved decisions in subsequent (though not identical) situations.

A computer program is said to learn from experience *E* with respect to some class of tasks *T* and performance measure *P*, if its performance at tasks in *T*, as measured by *P*, improves with experience *E*. (Sammut & Webb, G. I., 2011; Lantz, 2013).

Machine learning could also be used for dynamic and continuous authentication. User authentication is typically based on secrets that can be forgotten and stolen. Authentication normally is only done once, at the beginning of a session, and grants full access rights to a given identity. We envision a more flexible authentication scheme, which is potentially less prone to lost or broken secrets, using information stored about users on systems they log into, (Kloft & Pavel L, P., 2012).

Machine learning can use stored data to learn the behavior of legitimate users. Then, in some cases, users could authenticate simply by means of their usual actions, thus reducing the need for or bolstering traditional password-based authentication. Machine learning could strengthen passwords with questions derived from previous user activities (e.g., by inferring which acquaintances the user should reasonably be able to recognize based on their web-browsing). It similarly could also be used to generate secret questions for resetting forgotten passwords. Finally, it could provide for continuous and incremental authentication during the course of a session based on comparing user's activities with their profiles when users request additional privileges. (Biggio, Momin, Z., Fumera, Marcialis, & Roli, 2010; Beimel, Kasiviswanathan, & Nissim, 2012).

(Sommer & Paxson, V, 2010) indicated that machine learning methods are currently widely used as component in general reactive security architectures. They can optimally address targeted data-related security problems with clear semantics and well-defined scope. A key advantage of learning based approaches is their ability to generalize information contained in data, even though such generalization may not be easily expressible in a human-readable form. At the extreme, the generalization ability of

learning methods can even enable detection of previously unseen zero-day attacks, (Rieck, Trinius, P., Willems, C., & Holz, T, 2011).

While yielding excellent detection rates, learning methods occasionally may result in false alarms which can, however, be mitigated through appropriate tuning of detection thresholds. Another part of the "operational price" of learning-based approaches is the black-box nature of their predictions: even in the case when highly accurate detection is feasible, it is not always possible to identify the specific set of features that were "responsible" for these predictions. This limitation must be taken into account in their operational deployment (Meng & Kwok, L, 2013).

Given the proven success of learning-based approaches to narrowly focused security tasks, it is natural to expect that tight integration with existing security instruments may deliver substantial qualitative benefits. However, such integration is by no means a simple task. Machine learning algorithms can play a pivotal role here by potentially detecting completely novel, previously unseen attack samples. By providing confidence intervals for their predictions, learning methods can prioritize data to be manually inspected by experts and thus largely improve the productivity of these analysts (Sammut & Webb, G. I., 2011; Anthony, Pavel, L., Fabio, R., Tygar, D., & Blaine, N., 2014).

Integrated Solutions

This section looked into a combination of techniques because of the many limitations that the standalone possessed. Most approaches focus on detecting and filtering attack traffic near the target of the attack. The main limitation of this general approach is that the computational and network resources available to the attacker can readily exceed that of the target. This means that the zombies can engage in more complex transactions such as authentication requests or web queries, which are difficult to differentiate from

legitimate traffic. In order to respond to this growth in attack power, defenders need a more scalable approach to defense.

Compressed Anti IP Spoofing Mechanism Using Cryptography

(Gavaskar & Ramaraj, E, 2011), proposed a technique of IP spoofing using two way security mechanism compression and encryption. This was a method whose main objective of IP compression is to avoid the overhead, which provides the bandwidth utilization. The IP header compression work initiated ten years ago but still there is some drawback and problem persists. For handling the packet transformation in effective manner they moved to IPv6 but the header size would increase in IPv6. To increase the bandwidth utilizations, avoid the network traffic, congestion, collision, and then the compression technique was adopted. Basically compression was used to minimize the size of file into half. For example if the original file size is 100mb after compression it will reduced into 50mb here the files are decompressed without losing anything. Basic idea behind this was to remove the unwanted data's or information's.

The Global Resource Serialization algorithm was the novel algorithm that was designed for implementation. The concept behind this group of IP address is considered as a single no which is taken as host identification. The next step was applying the cryptography technique which was used because of its simple state. Simple functions in the implementation used transformation function as method. It just modified the one value into another form using add or multiply that value into original no. for example the previous 2 will converted onto 6 adding 4 with 2 . The final thing we have had to send the key value for decryption. Key value added into encrypted value for easy identification similar to the format of IP address 6.4 is the final value that was send to the destination machine likewise all 4tuple's. Again the decryption happened in reverse manner. Table 2.1 represents the algorithm used in Secure-Address Resource Protocol.

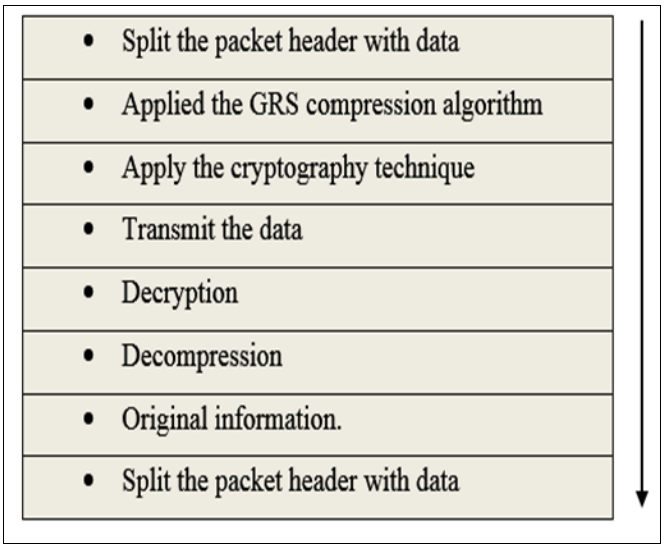

Table 2.1: Compression and Cryptography

(Gavaskar & Ramaraj, E, 2011)

Cryptography and Pretty Good Privacy (PGP)

Pretty Good Privacy (PGP) involves the process of cryptography. The PGP has commonly been used for electronic mails. According to (Zimmerman, 1995), PGP is a software that combined several high-quality; existing public-key encryption algorithms and protocols into one package for secure, reliable electronic mail and file transfer. The PGP concept was created by Phil Zimmermann in 1995 but did not have the unique techniques for encryption (Henry, 2000). Nonetheless, Rivest, Shamir, and Adleman (public key encryption technology), International Data Encryption Algorithm and digital signatures are the frequently used techniques for the encryption process in PGP at present.

(Shafinah & Ikram, M, 2011), the PGP is widely used due to several advantages it pertain which among them being a freeware, existence on web, and more secure algorithms. In addition, PGP is independent in view of the fact that it is neither in

extensive development, nor is it controlled by any government or organizational standards.

(Stallings, 2002), explained on five operations involved in PGP authentication, confidentiality, compression, email compatibility and segmentation. PGP uses an efficient algorithm that generates a hash code from the user's name and other information about the data to be transmitted. This hash code is then encrypted with the sender's private key. The receiver uses the sender's public key to decrypt the hash code. If it matches the hash code sent as the digital signature for the message, then the receiver is sure that the message has arrived securely from the stated sender.

Secure Address Resolution Protocol

(Bruschi, Ornaghi, A., & Rosti, E., 2003) used a new approach to prevent spoofing attacks by combining cryptography and Address Resolution Protocol (ARP) to make it more secure and increase results. Secure ARP (S-ARP) extends ARP with an integrity/authentication scheme for ARP replies, to prevent ARP spoofing attacks.

Since S-ARP is built on top of ARP, its specification (as for message exchange, timeout, cache) follows the original one for ARP. In order to maintain compatibility with ARP, an additional header is inserted at the end of the protocol standard messages to carry the authentication information. This way, S-ARP messages can also be processed by hosts that do not implement S-ARP, although in a secure ARP LAN all hosts should run S-ARP.

According to (Bruschi, Ornaghi, A., & Rosti, E., 2003), hosts that run the S-ARP protocol will not accept non authenticated messages unless specified in a list of known hosts. On the contrary, hosts that run the classic ARP protocol were able to accept even authenticated messages. A mixed Local Area Network (LAN) is not recommended in a production environment because the part running traditional ARP is still subject to spoofing attacks.

(Bruschi, Ornaghi, A., & Rosti, E., 2003), S-ARP uses asymmetric cryptography. Any S-ARP enabled host is identified by its own IP address and has a public/ private key pair. A simple certificate provides the binding between the host identity and its public key. Besides the host public key, the certificate contains the host IP address and the MAC address of the Authoritative Key Distributor (AKD), a trusted host acting as key repository. Each host sends its signed certificate containing the public key and the IP address to the AKD, which inserts the public key and the IP address in a local data base, after the network manager's validation.

Furthermore, the list of hosts not running S-ARP must be given to every secured host that has to communicate with an unsecured one. The interoperability with the insecure ARP protocol is given only for extraordinary events and should be always avoided. It is intended to be used only during the transition phase to a full S-ARP enabled LAN. A demonstration of the S-ARP is shown in figure 2.1

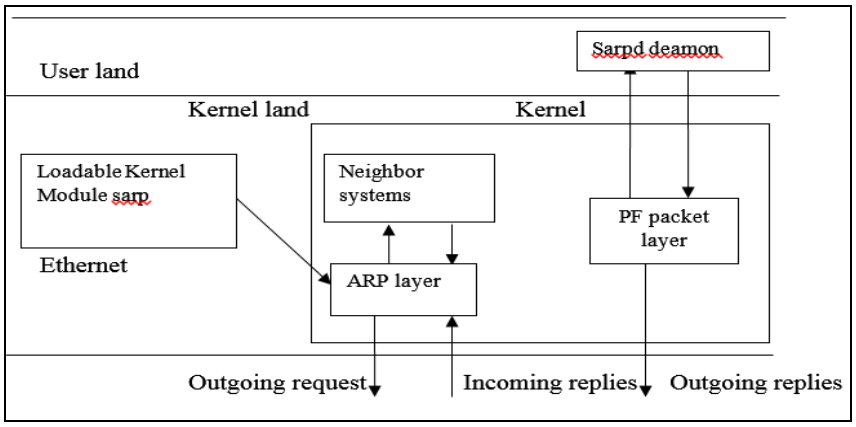

Figure 2.1: The structure of S-ARP.

(Bruschi, Ornaghi, A., & Rosti, E., 2003)

Desired Properties of Defense Mechanisms against Spoofing Attacks

A good solution to defend against these attacks should satisfy a number of properties brought forth by various scholars. (Ranjan, 2010; Zargar, Joshi, J., & Tipper, D. , 2013; Zhang, 2012). They include:

i. Fast response; the solution should be able to rapidly respond and defend against attacks. Every second of service disruption causes economic damage. As such the mechanism should be able to immediately mitigate the attack.

ii. Scalable; some attacks, involve only a small amount of packets, however, many spoofing attacks are large scale and involve large number of attack packets. A good defense mechanism must be effective against low packet count attacks but scalable to handle much larger ones.

iii. Victim filtering; almost all spoofing defense schemes assume that once the attack path is revealed, upstream routers will install filters in the network to drop attack traffic. This is a weak assumption because such a procedure may be slow, since the upstream ISPs have no incentive to offer this service to non-customer hosts and networks. Because large Internet servers are processing, not bandwidth, constrained, the servers themselves should be responsible for filtering out attack traffic that reaches them.

iv. Per-packet filtering: A defense mechanism against IP spoofing attacks should allow the victim to identify each individual spoofed IP packet so that legitimate packets can still be accepted.

v. Efficient; the solution should have very low processing and state overhead for both the routers in the Internet and, to a lesser degree, the victims of the attacks.

vi. Support incremental deployment: The solution is only useful and practical if it provides a benefit when only a subset of routers implement it. As an increasing number of routers deploy the scheme, there should be a corresponding increase in performance.

vii. Privacy; the deployment of the solution should not leak proprietary information about an ISP's internal network, as some ISPs keep their network topology secret to retain a competitive advantage.

Comparisons Between Integrated and Standalone Solutions

Review of standalone solutions and integrated solutions of eradicating spoofing attacks clearly indicates that integrated solutions perform better in comparison to their standalone counterparts. An example of the S-ARP show how cryptography enhances the performance of the normal ARP solution by including an authentication layer that the messages have to go through that requires a cryptographic key to decrypt in order to allow access leading to a more secure alternative in comparison to the normal ARP solution. S-ARP uses asymmetric cryptography. Any S-ARP enabled host is identified by it's own IP address and has a public/ private key pair. A simple certificate provides the binding between the host identity and its public key.

Another example is the compressed anti IP spoofing mechanism using cryptography uses the cryptographic feature to also assist in the encryption of the compressed header thus allowing only the data or messages that contain the decrypted key passage thus increasing security in comparison to the compressed anti IP spoofing mechanism that is standalone.

The same case applies to cryptography and pretty good privacy they are both independent methodologies but their combination makes them better performers. Pretty Good Privacy (PGP) concept is applied to increase the level of security for a digital file by enhancing security thus making it difficult for intruders by adding obstacles in order to obtain the files they desire. This is done by ensuring that an exact port number between client and server to add an obstruction for intruders trying to gain access. It increases security by applying of cryptography and compression processes. The intruders would have to necessitate more time period, additional methods and a specific

access key because of the difficulties when trying to access the files content as result of cryptography and compression.

Integrated solutions are a combination of two working standalone solutions and instead of having advantages of one methodology we get to have two methodologies working hand in hand to assist in complementing the other methodologies weakness or limitations. According to the literature review done cryptography is one of the most used solutions because it's more robust and can accommodate different methodology platforms. Various methodologies have been used to integrate with cryptography but no literature reviewed shows a combination with Stack Pi and encryption. Thus a solid reason why the choice of Stack Pi and Encryption seem like a valid combination to assist in the fight against spoof attacks.

Adoption of Stack Pi and Encryption Informed by machine learning

Combining source address authentication (to prevent IP spoofing), capabilities, and filtering would be the most effective and efficient solution because of the robustness of capabilities and the relative simplicity of a capability-based design, (Zargar, Joshi, J., & Tipper, D. , 2013).

The results of the combined techniques were an improved version of their standalone counterparts therefore complementing each other's strengths and weaknesses meaning more effective and efficient as an integrated solution. In review of all the standalone methodologies that we have seen for curbing of spoofing attacks, cryptography and StackPi stood out as the most effective and thus bound to give better results.

According to (Schneier, 2011), cryptography is one of the most important components of fraud prevention in all electronic money systems. Although it bears certain limitations as listed in its previous review it also bears a lot of weight and thus a perfect choice when it comes to integrating it with other methodologies. Encryption has been paired before with other methodologies giving outstanding results and thus there is guarantee

that if we integrate it with another powerful methodology it is to help bridge the gap that limits spoofing attacks.

Stack Pi originated from the *Pi*, a Path Identification algorithm but it had certain limitations which prompted the introduction of Stack Pi. According to (Perrig, Song, D., & Yaar, A, 2002), the original Pi marking is based on the use of the packet's Time to Live (TTL) field as an index into the IP Identification field where a router should add its marks. This method is not as lightweight as the StackPi method. Legacy routers have a harmful effect on the original Pi scheme because they decrement the TTL of a packet but do not add any markings. The StackPi scheme is robust to legacy routers and even includes the write-ahead scheme to incorporate markings for single legacy routers in the path.

Machine learning acts as a methodology for informing the two techniques for curbing spoofed attacks (Stack Pi and Encryption). It assists to update the filter table and learn the behavior of the attackers or attack packets and give a more informative solution before the attack happens. It used the rule based approach by allowing the researcher to create algorithms that enable the financial systems to train the data that is already in existence of previously spoofed sources and ensures that a repetition is not encountered. The rule based approach was the most suitable as it operates quickly, accurate and cheaply.

With the reviews a combination of these methods will mean an ultimate product that will not only curb spoofing attacks but will also enable the victim to track down the perpetrator involved in the action. This will guarantee an increase in the users of EPS systems confidence and thus they can perform their services to the best of their abilities saving both the supplier and the consumer billions of shillings in savings.

Summary

In this work standalone methodologies versus integrated solutions that are a combination of two working standalone techniques are presented. The researcher justified through a comparison of both solutions the added advantage that these integrated solutions possessed which supported the justification of the work that we underwent of integrating Stack Pi and Encryption as the methodologies of choice being informed by machine learning.

CHAPTER THREE

3.0 RESEARCH METHODOLOGY

3.1 Introduction

The methodology of this research examines Stack Path Identifier and Encryption as a good choice to be adopted as spoofing defense mechanism for EPS systems. The study was undertaken through a survey of financial institutions in Kenya, this is because the focus was on the supply side of electronic payment systems and the largest merchants for this systems are financial institutions. Relevant data was collected through questionnaires and extracts from existing records. Descriptive research was applied in the research. Data analysis was done through descriptive statistics obtained from SPSS (Statistical Package for Social Studies) V21. The data has been presented through bar-graphs, pie charts and tables. In order to meet the key deliverables the methodology was based on the study objectives.

3.1 Research design

A research design is a framework that guides the collection and analysis of data. A descriptive research design was used to collect both qualitative and quantitative data. A descriptive research survey as a method of research which gathers data at a particular point in time with the intentions of describing the nature of existing conditions of, or determining specific information. The data obtained from the study was analyzed and used to generate information in response to study objectives. The output of the data collected was instrumental to developing a proposed framework for the integration of the three selected methodologies, Stack Pi, Encryption informed by Machine learning.

3.2 Target population

A population is the total collection of element about which we wish to make some inferences. The target population consists of four major financial institutions within Nairobi County which have adopted EPS systems two of which were successful local banks and two were international banks with branches within the Nairobi County CBD. There was a total of 43 banks in Nairobi county that have adopted EPS systems. The reason for adopting Nairobi county is that it's the capital city of Kenya making it the epitome of business transactions thus a crucial target location for any foreign or local bank needing a market for its goods and services. This study population was justified on the basis that this are the institutions that have websites that deal with the most financial transfers and specifically the IT departments since they possess enough skills to understand the effects of spoofing on since they are the websites facilitators.

3.3 Sample Size and Sampling techniques

A sampling frame is the list of a group or a cluster which forms the basis of the sampling processes where a representative sample is drawn for the purpose of research. 10% of the target population of both the target bank population and IT technical and management respondents, is representative sampling frame for the research.

The study will use stratified random sampling technique. A stratification as the process of dividing members of the population into homogeneous subgroups before sampling. The study will use stratified sampling to select 2 local banks and 2 international banks that operate within Nairobi CBD. Stratified sampling will allow the researcher to target the most representative sample elements that are equipped with the knowledge about the intended phenomena.

Strata (St)	**Target Population (P)**	**Sampling Frame (SF) S=Px10%**	**Total Sample Size** **s=P(10%)**
Equity	30	3	3
Kenya Commercial Bank	30	3	3
Standard Chartered Bank	20	2	2
Barclays	20	2	2
Total	80		10

Table 3.1 Sampling Frame Technical Staff

Strata (St)	**Target Population (P)**	**Sampling Frame (SF) S=Px10%**	**Total Sample Size** **s=P(10%)**
Equity	10	1	1
Kenya Commercial Bank	10	1	1
Standard Chartered Bank	10	1	1
Barclays	10	1	1
Total	40		4

Table 3.2 Sampling Frame Management Staff

3.4 Data collection methods

The data collection methods used were primary and secondary sources. Questionnaires were the most appropriate form of data collection this is because it's both cost effective and saved a lot of time. The questionnaire contained both open and closed ended questions. Secondary data was extracted from sources provided by the respondents' organizations as well as from recent journals, articles, theses, papers and credible and reliable internet sources to for the purpose of references.

In order to determine the relationship that exists between the implementation of three anti spoofing defense mechanism (encryption, stackPI-IP and machine learning) and spoofing defense, for a period of five years (2010 – 2014) was considered because of the most recent development and current information accessibility. Scholarly articles, researches, annual statements, published printed sources, published electronic sources, government records and public sector records were used as sources of secondary data.

3.5 Data Processing

Primary data was analyzed through descriptive statistics (using SPSS V20) to provide an over view of respondents perception of the various aspects of the research objectives. Graphs, and histograms have been used where appropriate so as to ensure that the research findings are clear and easily understandable.

Once all the secondary data was collected, they were cleaned for errors. The data was then coded to allow response put into categories. After coding, data was classified according to common characteristics; these common characteristics were tabulated in a compact form by use of rows and columns for further analysis, comparison and explanations, the data then analyzed quantitatively by use of Statistical Packages for Social Science (SPSS) to interpret and explain the results of the study. In order to eliminate the possibility of obtaining false relationship, the study ensured that all the variables incorporated into the predicted model are clearly established, in the literature.

Regression estimates were derived using the simple ordinary least squares (OLS) method, statistically, least squares estimates are the most reliable regression estimates because of their general quality of minimized bias and variance.

The regression model is used by the researcher to demonstrate that the implementation of the three proposed mechanisms against spoofing attacks will lead to increased defense against spoofing attacks

3.6 Conclusion

The methodology selected involved the collection of primary data from technical and management respondents who supplied us with first hand data on their dealings with spoofing attacks. This data assisted in the development of a proposed framework that shows how the selected methodologies could complement each other and make a highly secure platform for defending spoofing attacks.

CHAPTER FOUR

4.0 DATA ANALYSIS, PRESENTATION AND INTERPRETATION

4.1 Introduction

This chapter presents the findings from a field survey conducted on April 2014 in Nairobi County. The chapter starts with descriptive statistics, including demographic characteristics of respondents. It also presents the results got from a linear regression done to identify how security influences the adoption of Electronic Payment Systems and the relation that Stack Pi and Encryption as a defense against spoofing attacks. The rest of the section has comparison of how a combination of techniques increases the results against spoofing in comparison to their standalone counterparts.

4.2 Response Rates

Financial Institution	Frequency	Percentage
Kenya Commercial Bank	4	29
Equity Bank	4	29
Standard Chartered Bank	3	21
Barclays	3	21
Total	14	100

Table 4.1: Response rates by organization

A total of 10 technical and 4 management staff responded to this survey from an initial target of 20 sample. That is 14 participants and 6 Non-participants, this occurred since most of organization do not have a lot of personnel in the I.T department.

The highest response came from our two local banks at 29% each followed by our two international banks 21%.

4.3 Demographic characteristics of respondents

The following is the demographic characteristics of respondents in relation to age of respondents, gender and years of schooling.

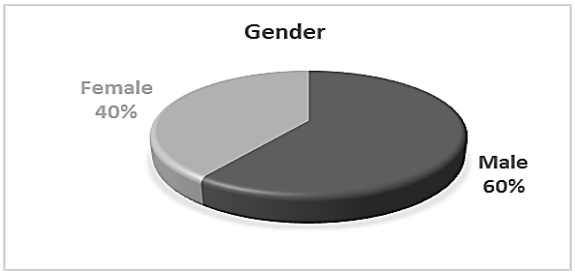

Figure 4.1: Gender of technical staff respondents

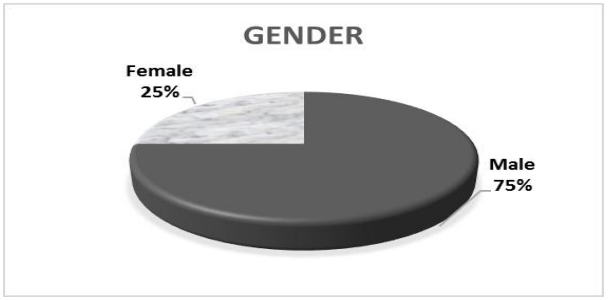

Figure 4.2: Gender of management staff respondents

Figure 4.1 shows that 60% of the technical staff respondents were male and 40% were female. Whereas figure 4.2 shows that 75% of the management staff respondents were male and 40% were female. This shows that the IT sector is more male dominated.

Education Level	Frequency	Percentage
Post graduate	2	20.0
Graduate	6	60.0
Middle Level college	2	20.0
Total	10	100.0

Table 4.2: Level of Education for technical staff respondents

Education Level	Frequency	Percentage
Post graduate	3	75.0
Graduate	1	25.0
Total	4	100.0

Table 4.3: Level of Education for management staff respondents

Table 4.2 shows that 20% of the technical staff respondents were post graduates, 60% graduates and 20% were middle level college graduates. Table 4.3 shows that 75% of the management staff respondents were post graduates, 25% were graduates. This illustrates a high level of academic competence that the respondents possess.

Position	Frequency	Percent
Technician	2	20.0
Technical Support	2	20.0
Website Support	2	20.0
Website Coordinator	4	40.0
Total	10	100.0

Table 4.4. Technical Staff Respondents Organizational Position

Position	Frequency	Percent
IT Manager	2	50.0
Chief Technology Officer	2	50.0
Total	4	100.0

Table 4.5. Management Staff Respondents Organizational Position

20% of the technical staff respondents held technicians positions, 20% were technical staff another 20% were website support and the remaining 40% were website coordinators.

As for the management staff respondents, 50% of them held the IT management position and the rest of the 50% were CTO.

Age	Frequency	Percent
25 and below	2	20.0
26-35	6	60.0
36-55	2	20.0
Total	10	100.0

Table 4.6. Technical Staff Age Group

Age	Frequency	Percent
25 and below	2	20.0
26-35	6	60.0
36-55	2	20.0
Total	10	100.0

Table 4.7. Management Staff Age Group

Table 4.6 represents the age of the technical respondents where 20% were 25 years and below, 60% were between the age of 26-35 years and the last 20% are between the ages of 36-55 years.

Whereas table 4.7 represents the age set of the management respondents where 20% are 25 and below, 60% were between the age of 26 and 35 and the remaining 20% were between ages 36 and 55. This shows that the greater percent is between 26 and 35 which represents 60% of the sample population.

Responsibility	**Frequency**	**Percent**
Hardware and software support	4	40.0
Website coordination	6	60.0
Total	10	100.0

Table 4.8: Management Staff Organizational Responsibility

Responsibility	**Frequency**	**Percent**
Technical management	2	50.0
Technical strategy management	2	50.0
Total	4	100.0

Table 4.9: Technical Staff Organizational Responsibility

Table 4.8 shows that 40% of the management staff respondents had the responsibility of hardware and software support and 60% did website coordination. Table 4.9 shows that 50% had the responsibility of technical management and the remaining 50% had the responsibility of technical strategy management.

4.4 Effects of spoofing attacks on adoption of online EPS systems

N	Median	Mean
10	1.0000	1.0000

Table 4.10: Use of online EPS system technical respondents

N	Median	Mean
4	1.0000	1.0000

Table 4.11: Use of online EPS system by management respondents

Table 4.10 and 4.11 show that all the respondents were in agreement that they used online EPS systems with a mean of 1.00 and a median of 1.00.

The results for both technical and management confirmed all the financial institutions did actually use online payment systems. In addition, the forms of online payments suggested by the respondents have been utilized by all the institutions. The three main forms of EPS payments that were represented were credit cards, website payment and mobile payments.

Type of EPS systems	**Rank**	**Frequency**
Credit cards	Yes	10
	Total	10
Website payments	Yes	10
	Total	10
Mobile payment	Yes	10
	Total	10

Table 4.12: Types of online payment systems by technical respondents

Type of EPS systems	Rank	Frequency
Credit cards	Yes	4
	Total	4
Website payment	Yes	4
	Total	4
Mobile payment	Yes	4
	Total	**4**

Table 4.13: Types of online payment systems by management respondents

4.5 Advantages of adopting online EPS systems

Figure 4.3 shows the advantages of online EPS systems as reported by the technical staff. A consensus shows that advantages one to four stated 70% of the respondents rated them as most favored and only the advantage increase in customer base differed where 30% of the respondents favored it, 50% were neutral and 20% less favored it. This demonstrates that the percentage of customers who adopted EPS systems was not as favorable as it should be considering the advantages one to four which the majority of respondents reported as most favored

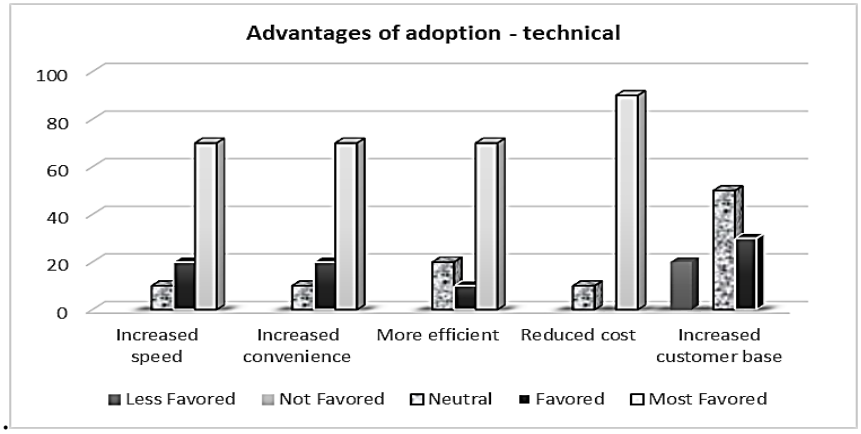

Figure 4.3: Advantages of adoption by technical respondents

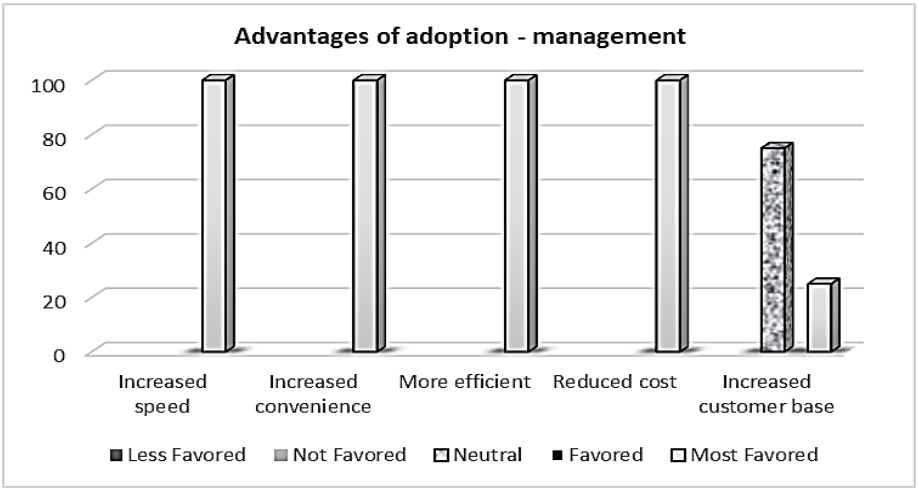

Figure 4.4: Advantages of adoption by management respondents

Figure 4.4 reports that all the management respondents rated advantages one to four as most favored and differed only on the customer base increase where 75% were neutral and only 25 % favored it. This confirms the trend that was displayed by the technical staff.

4.6 Awareness of spoof attacks

	Awareness of spoof attacks	Have you experienced spoof
N	10	10
Mean	1.0000	1.0000
Median	1.0000	1.0000

Table 4.16: Spoof awareness for technical respondents

	Awareness of spoof attacks	Have you experienced spoof
N	4	4
Mean	1.0000	1.0000
Median	1.0000	1.0000

Table 4.17: Spoof awareness and Experience for management respondents

Table 4.16 and 4.17 reports the mean and the median of both the technical and management respondents to be 1.000 meaning that they all were in agreement that they have experienced spoofing attacks.

4.6.1 Spoofing attacks encountered

Figure 4.5 reported that 50% and above of the technical respondents rated web spoofing, IP spoofing, email spoofing and TCP spoofing to be the most encountered spoof attacks. URL spoofing, MAC spoofing and DNS spoofing were rated to be less encountered in comparison to the rest having 60% and above of the respondents rating them as neutral encountered.

Figure 4.6 shows that the management respondents reported that web spoofing, IP spoofing, email spoofing and TCP spoofing ranked at 100% most encountered spoofing attacks .50% reported that DNS spoofing had 50% neutral and 50% encountered whereas 75% of the management respondents reported that MAC spoofing was the least encountered

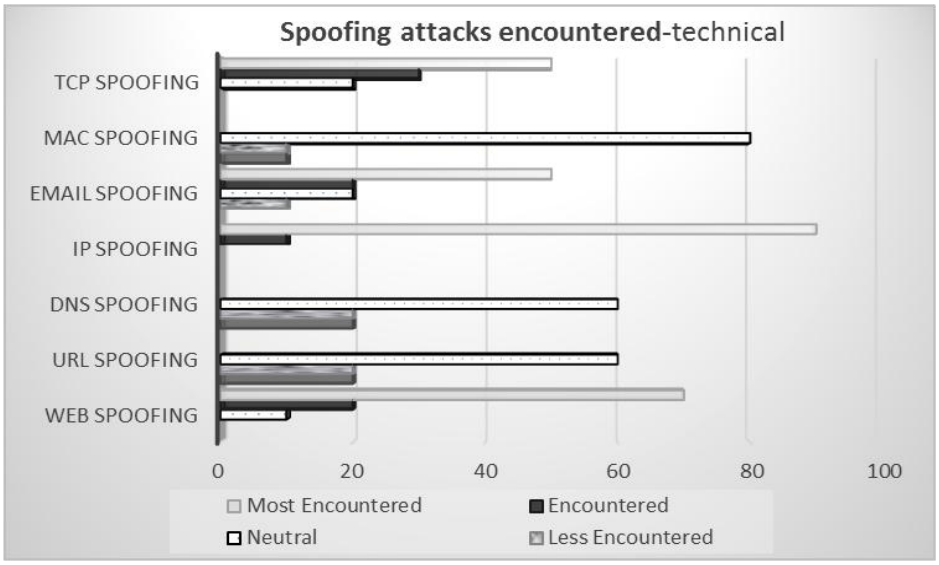

Figure 4.5: Forms of spoofing attacks encountered by technical respondents

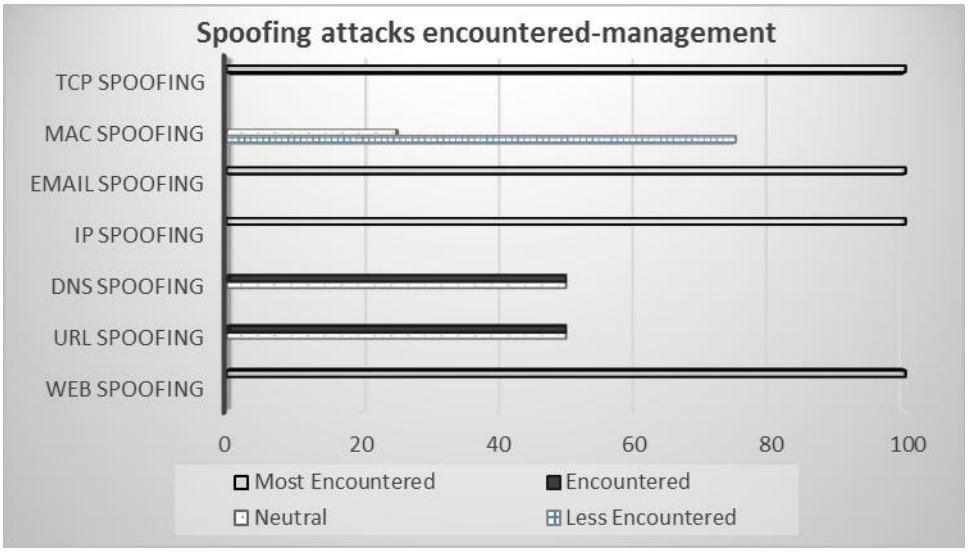

Figure 4.6: Spoofing attacks encountered by management respondents

4.7 Spoofing Attacks Negative Influence on Adoption and Procurement

Table 4.18 and 4.19 shows that both technical respondents and management respondents reported that spoofing attacks have a negative influence on adoption and procurement of EPS systems respectively.

N	Median	Mode
10	1.0000	1.0000

Table 4.18: Negative Influence on adoption

N	Median	Mode
4	1.0000	1.0000

Table 4.19: Negative Influence on procurement

4.7.1 Types of negative influences

Negative Influences	Ranks	Frequency	Percent
Denial of Services	Encountered	1	10.0
	Most Encountered	9	90.0
	Total	10	100.0
Cooperate Espionage and sabotage	Least Encountered	1	10.0
	Less Encountered	3	30.0
	Neutral	2	20.0
	Encountered	4	40.0
	Total	10	100.0
External Invaders	Encountered	2	20.0
	Most Encountered	8	80.0
	Total	10	100.0
Lack of consumer confidence	Encountered	1	10.0
	Most Encountered	9	90.0
	Total	10	100.0

Table 4.20: Negative influences as experienced by technical respondents

The negative influences that the technical respondents reported were such that more than 80% of them ranked denial of services, external invaders and lack of consumer confidence as the most encountered negative influences. Whereas 30% reported that corporate espionage and was less encountered, 20% reported it was neutral and the remaining 40% ranked it as encountered.

Negative Influence	Rank	Frequency	Percent
Denial of services	Most Encountered	4	100.0
	Total	4	100.0
Corporate Espionage and sabotage	Neutral	3	75.0
	Encountered	1	25.0
	Total	4	100.0
External Invaders	Most Encountered	4	100.0
	Total	4	100.0
Lack of consumer confidence on systems	Most Encountered	4	100.0
	Total	4	100.0

Table 4.21: Negative influences as experienced by management respondents

A similar trend is reported by the management respondents where 100% of them ranked denial of services, external invaders and lack of consumer confidence as the most encountered negative influences. Leaving corporate espionage and sabotage as a less encountered influence in comparison gaining a 75% neutral rank and the remaining 25% ranking it as encountered.

4.8 Techniques applied to curb spoofing attacks

N	Median	Mode
10	1.0000	1.0000

Table 4.22: Application of techniques by technical respondents

N	Median	Mode
4	1.0000	1.0000

Table 4.23 Application of techniques by management respondents

Table 4.22 and 4.23 show reports that both the management and technical respondents admit to have applied some techniques to help curb spoofing attacks.

4.8.1 Techniques successful

Techniques	**Rank**	**Frequency**	**Percent**
Network Ingress Filtering	Least Successful	9	90.0
	Less Successful	1	10.0
	Total	10	100.0
Distributed packet Filtering	Least Successful	3	30.0
	Less Successful	3	30.0
	Neutral	4	40.0
	Total	10	100.0
Cryptography	Successful	1	10.0
	Most Successful	9	90.0
	Total	10	100.0
ICMP Message traceback	Least Successful	3	30.0
	Less Successful	6	60.0
	Neutral	1	10.0
	Total	10	100.0
Hop count Filtering	Least Successful	6	60.0
	Less Successful	1	10.0
	Neutral	3	30.0
	Total	10	100.0
IP Traceback	Neutral	4	40.0

	Successful	6	60.0
	Total	10	100.0
Path Identification	Neutral	1	10.0
	Successful	6	60.0
	Most Successful	3	30.0
	Total	10	100.0
Cisco Netflow	Least Successful	9	90.0
	Less Successful	1	10.0
	Total	10	100.0
Stack Path Identification	Never used	10	100.0
	Total	10	100.0
Pushback	Least Successful	8	80.0
	Less Successful	2	20.0
	Total	10	100.0

Table 4.24: Successful techniques by technical respondents

Some of the techniques sampled by the technical staff were reported such that Network ingress filtering, ICMP message traceback, hop count and Cisco Netflow ranked as the least successful. Distributed packet filtering, IP traceback and Path Identifier were ranked as neutral in their success. 90% of the respondents voted cryptography as the most successful techniques with 10% voting it successful among the proposed and 100% of the respondents had not encountered Stack Pi as a technique of curbing spoofing attacks.

Techniques	Rank	Frequency	Percent
Network Ingress Filtering	Least Successful	1	25.0
	Less Successful	3	75.0
	Total	4	100.0
Distributed packet filtering	Neutral	3	75.0
	Successful	1	25.0
	Total	4	100.0
Cryptography	Most Successful	4	100.0
	Total	4	100.0
ICMP message for traceback	Least Successful	4	100.0
	Total	4	100.0
Pushback	Least Successful	2	50.0
	Less Successful	2	50.0
	Total	4	100.0
Hop-count filtering	Least Successful	4	100.0
	Total	4	100.0
IP traceback	Neutral	2	50.0
	Successful	2	50.0
	Total	4	100.0
Path Identification	Most Successful	4	100.0
	Total	4	100.0
Cisco Netflow	Less Successful	1	25.0
	Neutral	3	75.0
	Total	4	100.0
Stack Path Identification	Never used	4	100.0
	Total	4	100.0

Table 4.25: Techniques successful by management respondents

The same trend portrayed by technical staff respondents was duplicated by the management respondent, where 100% of the respondents voted encryption as the most successful techniques among the proposed and 100% of the respondents had not encountered Stack Pi as a technique of curbing spoofing attacks.

4.9 Weaknesses of the proposed techniques

Weaknesses	Rank	Frequency	Percent
Inadequate filtration	Yes	7	70.0
	No	3	30.0
	Total	10	100.0
Unknown attack source	Yes	10	100.0
	Total	10	100.0
Need for overhead services	Yes	4	40.0
	No	6	60.0
	Total	10	100.0

Table 4.26: Weaknesses experienced by technical respondents

Above 70% of the technical respondents reported that inadequate filtration and unknown attack source were the highest experienced weaknesses with needs for overhead services gaining a 40% vote as a weakness encountered.

Weaknesses	Rank	Frequency	Percent
Inadequate filtration	Yes	4	100.0
	Total	4	100.0
Unknown attack source	Yes	4	100.0
	Total	4	100.0
Need for overhead services	Yes	4	100.0
	Total	4	100.0

Table 4.27: Weaknesses experienced by management respondents

100% of the management respondents reported that inadequate filtration, unknown attack source and need for overhead services were weaknesses experiences reported to the management as experiences.

4.10 Comparison of combined techniques to standalone techniques

Application for combination	Ranks	Frequency	Percent
Technical respondents	Yes	4	40.0
	No	6	60.0
	Total	10	100.0
Management respondents	Yes	3	75.0
	No	1	25.0
	Total	4	100.0

Table 4.28: Attempt to combine techniques by both technical and management respondents

Table 4.28 shows that 40% of the technical respondents and 75% of the management respondents admitted to have attempted to combine some of the techniques used to curb spoofing attacks to gain better results whereas 60% reported of the technical respondents and 25% of the management respondents not to have attempted this technique.

4.10.1 Types of combined techniques

Combined techniques	Rank	Frequency	Percent
Cryptography+ARP	N/A	6	60.0
	Yes	2	20.0
	No	2	20.0
	Total	10	100.0
Cryptography+PGP	N/A	6	60.0
	Yes	1	10.0
	No	3	30.0
	Total	10	100.0
Cryptography+IP traceback	N/A	6	60.0
	Yes	1	10.0
	No	3	30.0
	Total	10	100.0

Table 4.29: Attempted combination as per technical respondents

Combined techniques	Rank	Frequency	Percent
Cryptography+ARP	N/A	1	25.0
	Yes	2	50.0
	No	1	25.0
	Total	4	100.0
Cryptography+PGP	N/A	1	25.0
	Yes	1	25.0
	No	2	50.0
	Total	4	100.0
Cryptography+IP traceback	N/A	1	25.0
	Yes	3	75.0
	Total	4	100.0

Table 4.30: Attempted combination as per management respondents

Among the attempted combinations reported to have been performed by both the technical and the management respondents it was visible that all the combinations proposed had the cryptography technique intertwined with another technique.

4.10.2 Advantages of combined techniques

Success factors	Rank	Frequency	Percent
Improved eradication of spoofing attacks	N/A	6	60.0
	Successful	1	10.0
	Most Successful	3	30.0
	Total	10	100.0
Less time consumed between identification and curbing process	N/A	6	60.0
	Neutral	2	20.0
	Less Successful	2	20.0
	Total	10	100.0
Better indicators for spoofing source	N/A	6	60.0
	Least Successful	2	20.0
	Less Successful	2	20.0
	Total	10	100.0

Table 4.31: Results of success as per technical respondent

Among the success of combining of techniques proposed, 30% of the technical respondents reported that improved eradication of spoofing attacks was among the most successful, whereas the success factor of having better indicators of the spoofing source got a rank of 20% least successful and 20% ranked it as less successful. The success factor of having less time between identification and curbing process had a rank of 30% neutral and 10% of the technical respondents ranked it as less successful.

Success factors	Rank	Frequency	Percent
Improved eradication of spoofing attacks	N/A	1	25.0
	Most Successful	3	75.0
	Total	4	100.0
Less time consumed between identification and curbing process	N/A	1	25.0
	Neutral	1	25.0
	Successful	2	50.0
	Total	4	100.0
Better indicators for spoofing source	N/A	1	25.0
	Neutral	1	25.0
	Successful	2	50.0
	Total	4	100.0

Table 4.32: Results of success as per management respondent

All the management respondents that had attempted a combination of techniques reported that improved eradication was the most successful factor, followed by less time consumed between eradication and curbing that was ranked as having a 50% vote on being successful and the remaining 25% ranked it as neutral. The success factor indicator of spoofing source had a rank of 25% neutral, and 50% reported they had had some success.

4.10.3 Limitations of combination

Limitations	Ranks	Frequency	Percent
Slower	N/A	6	60.0
	Yes	4	40.0
	Total	10	100.0
Couldn't indicate source	N/A	6	60.0
	Yes	4	40.0
	Total	10	100.0

Table 4.33: Limitations of combinations reported by technical respondent

Limitations	Ranks	Frequency	Percent
Slower	N/A	1	25
	Yes	3	75.0
	Total	4	100.0
Couldn't indicate source	N/A	1	25
	Yes	3	75.0
	Total	4	100.0

Table 4.34: Limitation of combination as per management respondent

Both the technical and the management respondents reported that the combined techniques had the limitation of being slower and also couldn't indicate the source of the spoof attacks.

4.10.4 Utilization of StackPi and Encryption combination

Combination of StackPi and Encryption	Ranks	Frequency	Percent
Technical respondents	No	10	100.0
	Total	10	100.0
Management Respondents	No	4	100.0
	Total	4	100.0

Table 4.35: Combination of Stack Pi and Encryption

Both the technical and the management respondents reported that they had not used Stack Pi and Encryption combination as a form of curbing spoofing attacks.

4.11 Regression analysis

The study looks at testing the relation between the three variables (stackPI-IP, encryption and machine learning) and defense against spoofing. To do this the researcher conducted a regression analysis and the idea here is that to determine if these security mechanisms have impact on defense against spoofing individually and combined, the intercept of the regression will be high for spoofing defense. R square and t-test at 95% confidence level was estimated. The study uses regression for the following reasons:

1) To establish a relationship between dependent variable and independent variable.

2) The dependent variable is random in nature hence the regression would aim to establish a relation between the security types and profitability.

3) The study uses the following regression equation to predict the dependent variable:

$$Y=\beta_0+\beta_1X_1+\beta_2X_2+\beta_3X_3+\varepsilon \quad \text{.....(5.1)}$$

Where:

Y= Dependent variable

β_0 = Intercept

$\beta_1 \ldots$to β_3 = Are the coefficient of the variables

X_1= Encryption

X_2= StackPI-IP

X_3= Machine learning

ε = Error term.

The study makes following assumptions about the data in order to conduct regression: The study assumes a relation between the dependent and the independent variables, the independent variable is categorical in nature, and the residuals in the model are random and normally distributed with a mean of zero (that is they are random). R^2 and t-test at 95% confidence level were estimated.

4.11.1 The relationship between Encryption and Spoofing Defense

Model Summary

R	R Square	Adjusted R Square	Std. Error of the Estimate
.577	.507	.211	2.610

The independent variable is Encryption.

Table 4.36: Model summary of encryption and spoofing defense

Adjustable R square is called the coefficient of determinant and tells us how the spoofing defense varies with variation in encryption implementation. From the table above, the value of the R-Square indicates that only 50.7% of overall spoofing defense is attributed to encryption implementation (including scheme). The adjusted R-Square of 0.211 however indicates there was a variation spoofing defense that is determined by

other factors. This means that there is significant relationship between encryption adoption and the spoofing defense.

Coefficients

	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
Encryption	2.30	.020	.577	1.224	.308
(Constant)	1.687	2.912		.267	.807

The independent variable is encryption.

Table 4.37: Coefficient results of Encryption and Spoofing Defense

The table 4.37 means that spoofing defense is not totally dependent on the encryption. Even if encryption is not implemented there would still be some level of defense against spoofing that is attributed to other approaches. The coefficient of encryption is 2.30 indicating that the type of encryption scheme contributes positively to spoofing defense thus a positive relationship between the encryption scheme and spoofing defense. The t-test indicates that the spoofing defense dependence on encryption is significant. The test of significance indicates that the coefficient of 2.30 in the case of encryption, meaning that there is a significant association between spoofing defense level and encryption scheme. In general, the type and implementation method of the encryption scheme determines the defense level.

4.11.2 The relationship between StackPI-IP and Spoofing Defense

Model Summary

R	R Square	Adjusted R Square	Std. Error of the Estimate
.584	.341	.121	1.063

The independent variable is stackPI-IP.

Table 4.37: Model Summary of StackPI-IP and Spoofing Defense

From the table 4.37 above, the value of the R-Square indicates that 34.1% of the spoofing defence is attributed to stackPI-IP. The adjusted R-Square of 0.121 indicates the level of spoofing defence, meaning that 12% of defence against spoofing are attributed to stackPI-IP.

Coefficients

	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
stackPI-IP	1.283	.019	.584	1.246	.301
(Constant)	.667	.595		.365	.739

The independent variable is stackPI-IP.

Table 4.38: Coefficient results of StackPI-IP mortgage and Profitability

Table 4.38 shows that the coefficient of variable StackPI-IP 1.283 indicating that the stackPI-IP contributes positively to spoofing defense. The test of significance indicates that the coefficient of 1.283 in stackPI-IP, meaning that there is a significant association between spoofing defense level and stackPI-IP.

4.11.3 The relationship between Machine Learning and Spoofing Defense

Model Summary

R	R Square	Adjusted R Square	Std. Error of the Estimate
.468	.219	.104	16446773.900

The independent variable is machine learning.

Table 4.39: Model summary of Machine Learning and Spoofing Defense

From the table 4.39 above, the R-Square value indicates that only 21.9% of the spoofing defense are explained by machine learning. The adjusted R-Square of 0.104 indicates,

this means that there exists a significant relationship between machine learning adoption and spoofing defence.

Coefficients

	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
machine learning	1.210	.022	-.468	-.844	.427
(Constant)	2.542	2.210		-.464	.674

The independent variable is machine learning.

Table 4.40: Coefficient results of machine learning, and spoofing defense

The table 4.40 indicates that machine learning influences spoofing defense. The coefficient of machine learning 1.021 in this case spoofing defense; as such there exists a significant relationship between the machine learning and spoofing defense.

4.11.4 The relationship between Encryption, StackPI-IP, Machine Learning, and Spoofing Defense

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.784[a]	.715	.539	3.124

a. Predictors: (Constant), Encryption, StackPI-IP, Machine learning

Table 4.41: Model Summary of the three variables and spoofing defense

From the table 4.41 above, the R-Square indicates that only 71.5% of spoofing defense are explained by encryption, stackPI-IP, machine learning, and spoofing defense. The adjusted R-Square of 0.539 indicates that the three variables have significant relationship and therefore defense positive effect on spoofing.

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.909	.256		1.280	.826
	Encryption	1.108	.192	2.608	1.564	.673
	StackPI-PI	1.027	.142	.676	1.192	.880
	Machine learning	1.121	.143	-2.747	1.844	.554

Dependent Variable: spoofing defense

Table 4.42: Coefficients Summary of the three variables and spoofing defense

The regression model arising from the above data is of the form

$$Y=2.909+1.108X_1+1.027X_2+1.121X_3 \quad \text{.....(5.2)}$$

The above regression model, indicates that spoofing defense with a constant defense of 2.909. Upon implementation of encryption spoofing defense would increase by a factor of 1.08, stackPI-IP by a factor of 1.27 and machine learning 1.121. This means that the implementation of the three spoofing defense mechanisms would have a significant positive influence on spoofing defense, which in practice could be increased by optimum, efficient and effective implementation.

4.12 Conclusion

The study shows that among the technical and management respondents the majority were young below 55 years and had attained a high level of education. It also emphasizes that all the respondents do recommend the usage of EPS systems indicating the various advantages experienced by each individual. In addition it indicates the respondents' awareness of the presence of spoofing attacks in their systems and it's the negative influence that these spoofing attacks have on adoption and procurement of the EPS systems.

The study also discussed some of the spoofing attacks experienced by this individuals and a couple of the methodologies that were used to eradicate them. Most of the respondents admitted to have used one or several of the methodologies in their quest to curb spoofing attacks. In addition during the pretesting of the questionnaire an additional column of NEVER USED was added to cover the methodologies that were proposed but had never been implemented before.

An introduction of combining methodologies as a stronger tool in comparison to the standalone counterparts showed that majority of the respondents viewed it as a novel concept and had not implemented it in their organization but concluded that all the respondents would like to try it. The minority that had experienced integration of some of the methodologies had confirmed that there were significant advantages in combining the methodologies and the results they experienced were highly impressive in comparison to their standalone counterparts. They also admitted that although the combination was effective some limitations that were notable had been experienced and a proposal was made for a research should to be performed to check for solutions.

Lastly, the regression analysis, indicated a clear association between the techniques proposed (Stack Pi, Encryption and Machine Learning) and their effects on spoofing attacks indicating that each had a crucial role to play in the defense against spoofing attacks.

CHAPTER 5

5.0 PROPOSED CONCEPTUAL FRAMEWORK

5.1 Proposed Framework

The research proposed a framework with the integration of Stack Pi, Encryption informed by machine learning. The information collected from the technical and management respondents aided in developing an integrated solution for spoofing attacks and with the most outstanding standalone techniques (Stack Pi, Encryption and Machine Learning) from the primary data assembled.

(Zargar, Joshi, J., & Tipper, D. , 2013) established that combining source address authentication (to prevent IP spoofing), capabilities, and filtering would be the most effective and efficient solution because of the robustness of capabilities and the relative simplicity of a capability-based design. Figure 5.1 shows a combinational framework adopted as a defense mechanism against spoofing attacks.

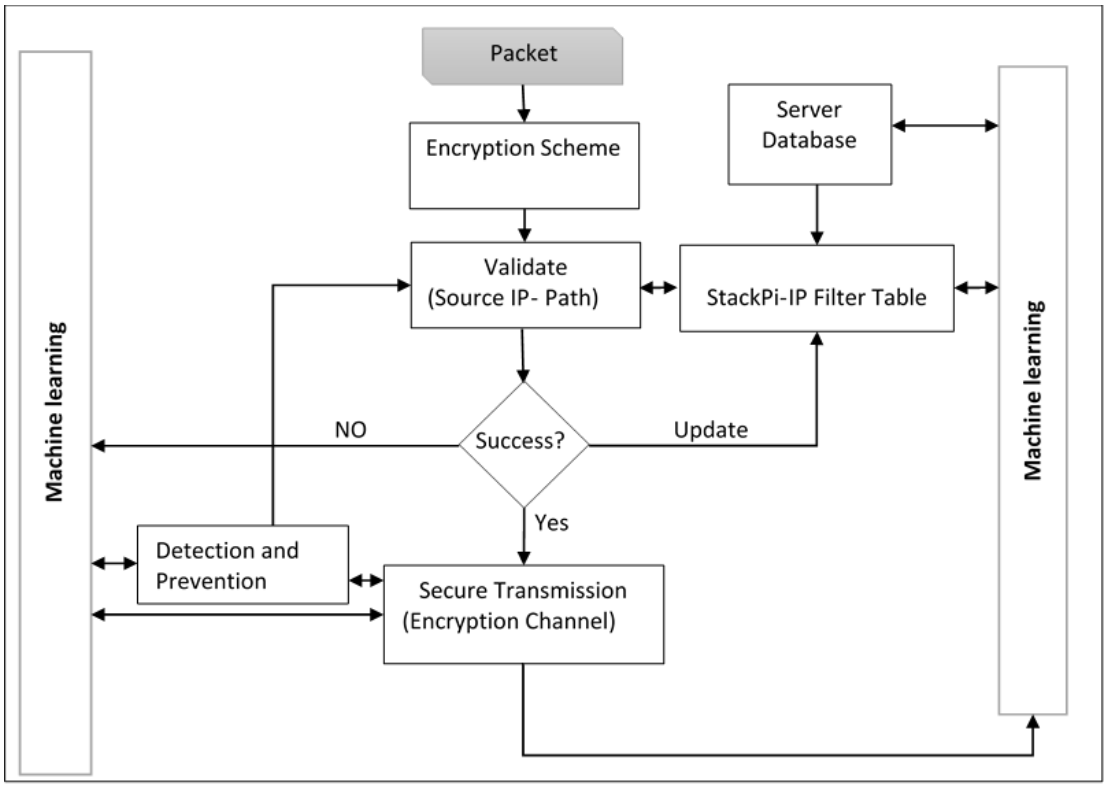

Figure 5.1: Proposed Framework

5.1.1 How it Works

In this framework, a hash code encryption scheme is assumed, however, the encryption scheme should be predetermined by the financial institution and should be enforced at both ends. This encryption is used to reduce collisions among packet-markings.

In brief, this is how the framework works; encryption is done for source IP Address into fixed-length hash code using hash function and placed into Identification field of IPv4 Header and sent packet into the network. A hash function is applied by the receiver to the source IP Address to produce hash code which is compared to the hash code available in Identification field. If both hash codes are equal then packet is authenticated.

If source IP Address of packet modified in network by an attacker than hash code will not be equal and recipient flags that packet. Further, the packets path is validated using marking (stackPi-IP) and detection schemes (informed by machine learning) source is verified and packet is validated. Once packet and source address is validated then the packet is transferred for better detection and prevention of spoofed attack using machine learning, then the filter table is updated accordingly. The time required to mark each packet is saved because in this framework, once a secure transmission is established between source and destination then there is no requirement of marking and comparing process at participant routers and firewall router respectively.

If it is first time communication between sender and receiver then with the help of marking and detection schemes source is verified and packet is validated. The researcher proposes that the stackPi-IP filter table use two filter tables; filter-in and a blacklist (also regarded as drop list) table. The filter-in table consists of legitimate user's paths and IPs, the drop list on the other hand consists of known threats and their subnets whose attempted communication with the network is just dropped; by dropping it means will be silent in its denial, that is, the connection will be rejected but the initiator will assume that no service is running on the target host (or that target host does not exist). During the entire cycle of the framework it interacts with machine learning which tracks and learns packet behavior, the database filter table and checklist are consequently updated.

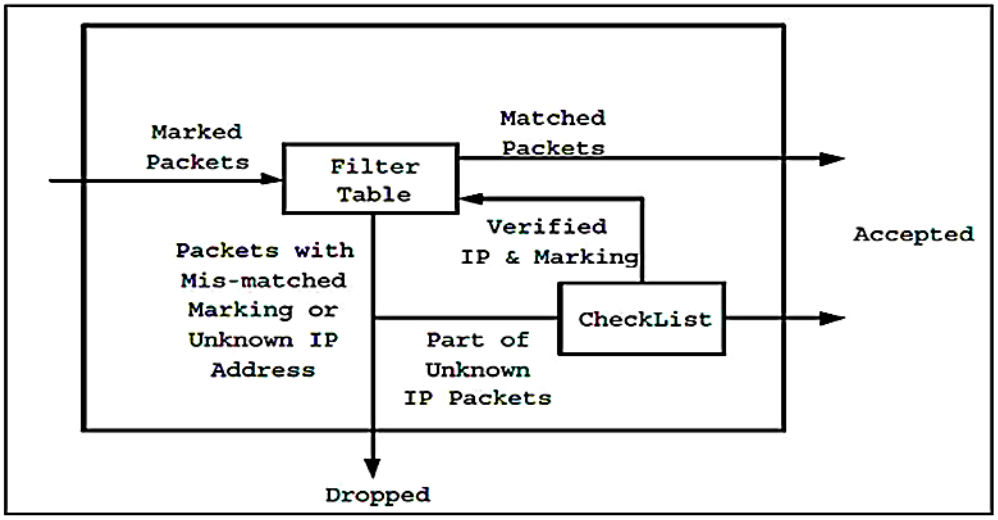

Figure 5.2: Stack Pi Marking scheme

The Hashed encryption scheme employs a firewall at each of the perimeter routers of the network to be protected and scans the marking field of all incoming packets to selectively filter the attack packets. (Bangar, Mulani, J.A, Ekad, A.B, Ganjewar, P.D, & Shinde, P, 2012). On implementing the StackPi marking any packet arriving at the network is marked depending only on the path it has traversed. If the source IP address of a packet is spoofed, this packet must have a marking that is different from that of a genuine packet coming from the same address. The spoofed packets can therefore be easily identified and dropped by the filter, while the legitimate packets containing the correct markings are accepted.

The filtering sequence is such that If the (stackPi-IP) tuple is same with one of the records in the Filter Table, the packet is received; If the source IP address of the packet exists in the Filter Table, but the marking does not match, this packet is considered to be a spoofed packet and is dropped, the path and if possible subnet is blacklisted, filter table updated. If the source IP address does not appear in the Filter Table, then this packet is accepted securely for detection and prevention after which the packets will either be dropped or accepted. All echo reply messages that are received as responses to the

firewall's requests are handled by the Check List verification process. They are not passed through the filter.

5.1.2 StackPI

In StackPi, as a packet traverses routers on the path towards its destination, the routers deterministically mark bits in the packet's IP Identification field. The deterministic markings guarantee that packets traveling along the same path will have the same marking. StackPi allows the victim and routers on the attack path to take a proactive role in defending against spoofing attacks by using the StackPi mark to filter out attack packets on a per packet basis. In addition, the victim can build statistics over time relating StackPi marks to IP addresses. Then if an attacker spoofs an IP address, it is likely that the StackPi mark in the spoofed packet will not match the StackPi mark corresponding to the legitimate IP address in the database, thus enabling the victim to tag packets with possibly spoofed source IP addresses. StackPi is also effective against other IP spoofing attacks such as TCP hijacking and multicast source spoofing attacks. (Das, Janahanlal, S, & Yogesh, C. , 2011; Gupta & Kavyashree, H, 2013).

Pi reuses the fragmentation field of an IP packet to identify the path the packet traveled. As a packet travels the network, each router it encounters sets a bit in the fragmentation field. When the packet reaches its destination, the fragmentation field will contain a marking that is (almost) unique to the path the detection, (Soon, 2012).

5.1.3 Packet Filtering (StackPi-IP Filtering Mechanism)

According to (Perrig, Song, D., & Yaar, A, 2002), StackPi allows for per-packet filter decisions and is geared to defend against spoofing attacks, it is extremely important that the filters at the endhost have a low per packet computation cost, as an endserver will need to be able to filter every packet that arrives over the network.

For the stackPi filtering design the researcher proposes the use of stackPi-IP filtering design indicated that packets from a given IP network will all arrive at the destination with a small number of distinct Pi marks, we can use this to design a powerful filter to reject packets with spoofed IP addresses.

Consider the following setup; during peace time (when a server is not under attack), the server stores the tuple <Pi mark, source IP address>, or (<Pi,IP>). When the server is under attack, it uses the <Pi,IP> database to filter out packets with spoofed source IP addresses. For each incoming packet, the server checks whether the < Pi,IP> tuple of the arriving packet matches an entry in the database; if the tuple does not match the corresponding entry in the database, it rejects the packet.

According to (Perrig, Song, D., & Yaar, A, 2002), a nice feature of this PiIP filter is that the server can filter out the very first malicious attacker packet. However, the forwarding path of a legitimate receiver may change and the arriving packet's <Pi,IP> tuple may not be in the database. Thus, the application writer needs to consider the output of the PiIP filter as a hint on whether the source IP address is spoofed or not. As long as the server has sufficient capacity, questionable packets may also get served, and if the packet originator turns out to be a legitimate user, the server can add the <Pi,IP> tuple to its database. Note that the PiIP filter cannot be used to detect IP spoofing attacks if the IP address in the packet is not in the database. However there are several ways to address this issue. Because packets from the same network (even if not from the same IP addresses) usually have the same Pi mark, from the Pi mark of one IP address we can derive the Pi mark of other IP addresses on the same network, this is also where machine learning comes in.

(Song, 2002), the StackPi filtering extremely light-weight and efficient, but here it presents a slightly more complex but more accurate filtering method. The filter itself is simple; examine an incoming packet's StackPi mark and source IP address and allow access based on that tuple. Ideally, a database of legitimate users' *h* Stack *Pi, IP i* tuple

will be built during times when there are few or no ongoing attacks. Any packet with a StackPi marking that does not match the StackPi marking of the same IP address in the database will be flagged as a packet with a spoofed IP address.

(Perrig, Song, D., & Yaar, A, 2002), in the case of filtering based only on StackPi markings, we have to assume that our filters get feedback from some higher layer algorithm that can classify some sampled packets as legitimate packets or attack packets, and tell the filter which StackPi markings correspond to attack traffic and should be dropped. The StackPi-IP filter does not rely as strongly on this assumption, because the StackPi-IP filter does not need to be bootstrapped with attack traffic. Quite the opposite, the StackPi-IP filter is bootstrapped during non-attack periods and identifies attack periods by an increase in the incidence of packets with spoofed IP addresses. We define the set of *n* distinct StackPi markings recorded for address *k* as *{m0,m1.....;mn}*. For each Stack Pi mark recorded at the victim for IP address *k*, there is a set of other IP addresses that also map to the same StackPi mark. If the attacker were to spoof any of these, the attack packet would be accepted by the filter. Thus, the probability of an attacker with IP address k successfully spoofing is:

$$P_k = \frac{\sum_{i=0}^{n} uniqueIPs(m_i, k)}{N} \quad \text{.....(5.1).}$$

Adopted from (Perrig, Song, D., & Yaar, A, 2002)

Where, the unique IPs function returns the number of unique IP addresses that map to Pi mark mi, excluding IP address *k* as well as any duplicates between function calls, and *N* represents the number of end-hosts in the topology; which is the size of the list of possible IP addresses that the attacker can spoof. Given the probability of an attacker with a specific IP address of successfully spoofing a packet, we can now calculate the probability of an attacker with a random IP address successfully spoofing:

$$P = \frac{\sum_{k=0}^{N} P_k}{N}$$ ……. Equation 5.2.

Adopted from (Perrig, Song, D., & Yaar, A, 2002)

Numerous research in real topologies have shown that an attacker has a very small chance to successfully spoof another IP address that is not from the same network as the attacker.

5.1.4 Enabling Traceback with StackPi-IP filters

A properly bootstrapped StackPi-IP filter in conjunction with machine learning can be used to perform standard traceback, that is, complete path reconstruction from a packet's destination to its sender. When a destination receives a packet that is flagged because its source IP address does not match its StackPi marking in the StackPi-IP filter's database, the victim can consult its database to generate a list of IP addresses that correspond to the packet's StackPi mark. Once this list is compiled, the victim can determine the paths by simply executing *traceroutes* to the addresses on the list. Although this method does not guarantee a unique path to the sender (because there may be multiple IP addresses that map to the same StackPi mark), it does reduce the space of potential attackers and may allow the victim's administrator to cull the true attack path using external knowledge and intuition; machine learning could also be used to enhance traceroute, Dehmer and Basak (2012).

5.1.5 Encryption

Implementing encryption and authentication will also reduce spoofing threats this is further enhanced by ensuring that the proper authentication measures are in place and carried out over a secure (encrypted) channel. With the help of cryptosystem we can enhance the speed of detection and prevention of IP spoofed packet.

Rather than doing the marking for each packet after confirmation of source validity, if further packet transmission is required the packet is put in secure transmission with cryptosystem. It would be more reliable that source address of IP packet should be encrypted.

The researcher proposes that financial institutions select an encryption schemes that best suits them. To understand how this works better consider a hash encryption scheme; encryption is done for source IP Address into fixed-length hash code using hash function and place this hash code into Identification field (of IPv4, this is also applicable in IPV6) header and send that packet into the network. On the other side, recipient receives that packet and applies hash function to the source IP Address to produce hash code and compare this hash code to the hash code available in Identification field. If both hash code are equal then packet is authenticated. If source IP Address of packet modified in network by an attacker than hash code will not be equal and recipient discard that packet.

At sender side source address of sender inside generated packet is used to generate the hash code with the help of any known hashed algorithm. This hash code is written in to the identification field of the packet, then the IP packet is transferred by usual method. Whenever IP packet is received at receiver side if it is first time communication between sender and receiver then with the help of marking and detection schemes source is verified and packet is validated. Once packet and source address is validated then the packet is transferred for better detection and prevention of IP spoofed attack using machine learning then the filter table and checklist is updated accordingly. All these measures are carried out over a secure (encrypted) channel.

The time required to mark each packet is saved because in this framework once a secure transmission is established between source and destination then there is no requirement of marking and comparing process at participant routers and firewall router respectively.

5.1.6 Machine learning as an integrated technique

Machine learning incorporated in this framework to address the short comings of StackPi-IP filtering method and thereby increasing its efficiency. In machine learning this is done via three approaches:

(Perrig, 2002), Firstly, by inferring StackPi markings of previously unseen IP addresses. We observe that for a given destination, all the packets originating from the same network region (sometimes from the same CIDR block) will usually be routed along the same path and have the same StackPi marking. If we have seen a StackPi mark from a given network, we could infer the StackPi marks of other hosts within the same network. To ensure we reliably derive information about hosts that are on the same network we will consider using the CIDR block information from BGP routing, and using machine learning techniques in conjunction with longest prefix matching of IP addresses with their associated StackPi marks.

(Yaar, 2002), Secondly, by inferring multiple StackPi markings in case of multi-path or short path. For a given destination, if a region has multiple paths to the destination, then the StackPi marking of any host within that region may have multiple values. For example, given two hosts, A and B, from the same region, and whose StackPi marks are X and Y, respectively, then it is likely that the StackPi marking of A could also be Y, and the StackPi marking of B could also be X. We could use machine learning techniques to automatically detect this case and infer the multiple StackPi markings from observed data. In the case where some bits in the StackPi mark still contain the original bits of the IP Identification field, research has shown that the StackPi markings have the same low order bits (from router markings pushed onto the stack) and only vary in the high-order bits (those bits that were not overwritten by router markings). Using machine learning techniques, we could automatically detect this case and filter only based on those bits that were not originally in the IP Identification field.

(Song, 2002), Thirdly, by inferring StackPi marking change caused by route change. When routes change, StackPi markings will change for some end-hosts. Because packets from the same region will have the same StackPi markings, the change of StackPi marking for one IP address will have a similar change for another IP address from the same region. Using machine learning techniques we could infer the StackPi marking change caused by a route change with a small number of packets. Also, with machine learning techniques, we may be able to infer how route changes affect the StackPi markings and hence infer the StackPi marking change of one network region by observing the StackPi marking change of another network region.

5.2 Proposed Framework Evaluation

The proposed framework presents advantages as the integrated approach ensures the different methodologies complement each other and presents several advantages including; ensuring high speed filtering of spoofed packet, enhancement in packet transmission, and once secure transmission is established no role of participating router in filtering process.

(Perrig, Song, D., & Yaar, A, 2002), used skitter maps and internet map to do the analysis indicated the expected values of the proposed framework performance effectiveness against random strategy selection (indicated by stackPi Non-users). The figures (which figures? Better use "the results…) indicate a significant difference in performance with the proposed framework being better. For instance, even before the introduction of encryption and machine learning in figure 5.3, when attack traffic is 160 times user traffic (in the attack scenario of 500 users and 8000 attackers), 50% of the server's capacity is utilized for servicing legitimate user's packets when using the StackPi filter, while only 0.6% of the server's capacity is used to serve legitimate user's packets when the server uses a random selection strategy. Also worth noting is the significant improved performance with the introduction of encryption and machine learning figure 5.4.

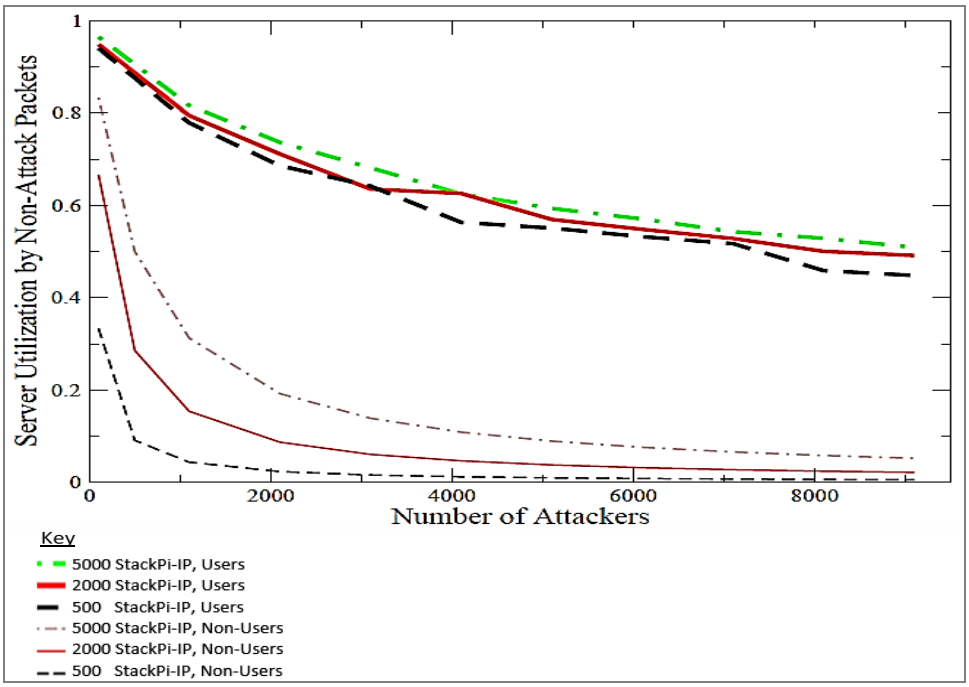

Figure 5.3: StackPi-IP number of attackers against server utilization

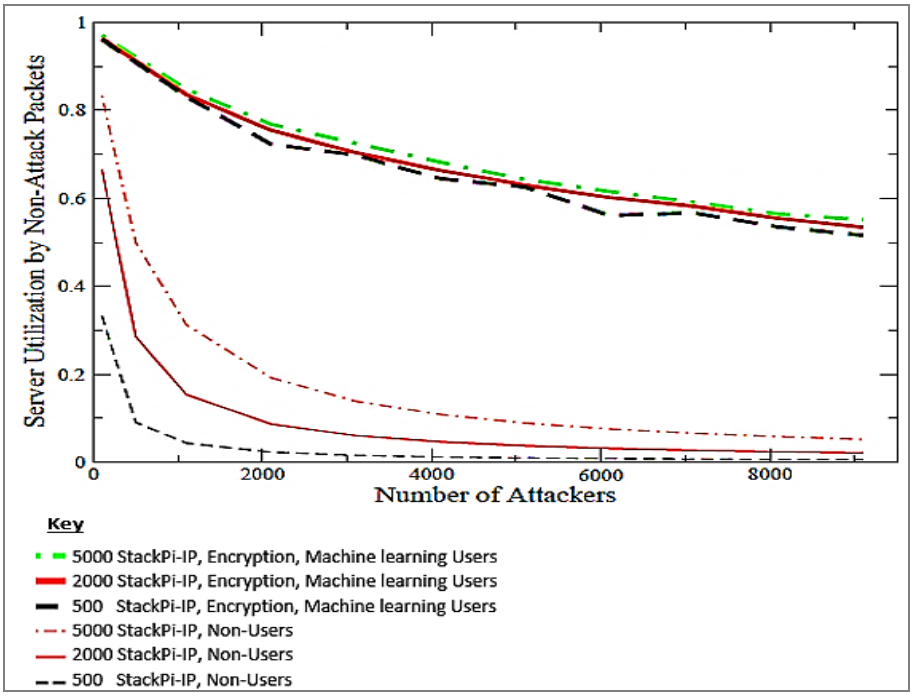

Figure 5.4: Combined approach number of attackers against server utilization

Sensitivity analysis is the study of how uncertainty in the output of a model can be attributed to different sources of uncertainty in the model input. The sensitive variable is modeled as uncertain value while all other variables are held at baseline values (stable).

A sensitivity analysis was done to determine correlation between the factors that are desired in defense mechanism against spoofing attacks and our approach. As indicated in the table 5.1, if properly implemented the proposed framework has all the desired properties; with filtering (both per packet and victim being its major strength) with expected values of 11.45 and 10.03 respectively, the ability for scalability in deployment and efficiency are also some of the characteristics portrayed by the framework. Privacy ranks low but at acceptable level, this could be attributed to the fact that privacy is a result of various factors and is very relative, however this can be improved.

		StackPi-IP		
		Expected Value	Variance	S.D
Desired Properties	Per-packet filtering	11.45	324.211	18.006
	Victim filtering	10.036	178.663	13.366
	Incremental deployment	8.801	138.77	11.78
	Efficient	6.802	77.904	8.826
	Fast response	7.126	85.125	9.226
	Scalable	5.128	46.983	6.854
	Privacy	4.252	26.457	5.144

Table 5.1 : Sensitivity analysis: StackPi | Desired properties

5.3 The Framework Simulation

Simulation results were obtained by use of AgenaRisk Bayesian Network software, which uses the latest developments from the field of artificial intelligence and visualization to solve complex, risky problems. To evaluate the proposed framework the research used analyzed secondary data to determine the relationship between the study variables from numerous studies conducted on and by financial institutions spanning the last five years. Additionally, confidential primary data from financial institutions in Kenya were used.

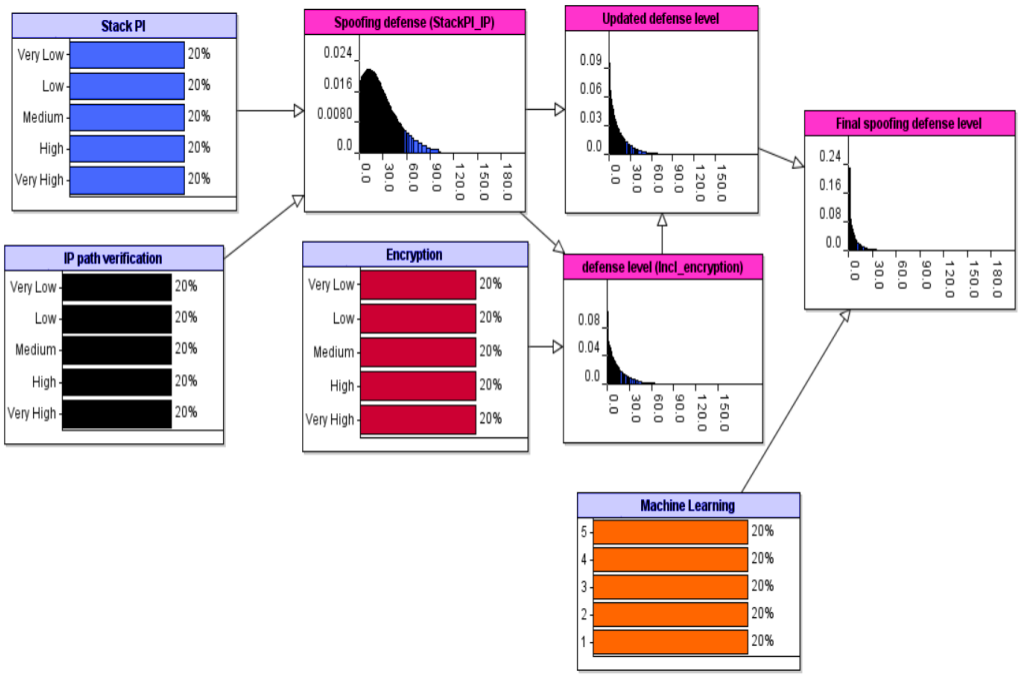

Figure 5.5: Initial Framework Simulation

The initial simulation assumes an even distribution on the implementation of the defense approache efficiency; each with an equal chance of its efficiency varying from very high to very low. In this regard after the implementation of StackPI-IP, the spoofing defense level indicated by the risk level has a mean of 2.16; after implementation of encryption this level drops to 14.15. The framework being iterative, some changes are expected to

be made based on the new implementation (encryption), the initial defense implementations and risk levels leading to the updated defense level. On inclusion of machine learning in the framework, using a five point scale of 5 being highly effective and 1 being highly ineffective, the final spoofing defense level significantly drops to a mean 7.15.

Entering several scenarios into the model sheds more light into the relationship between the research variables and their effect on defense against spoofing attacks.

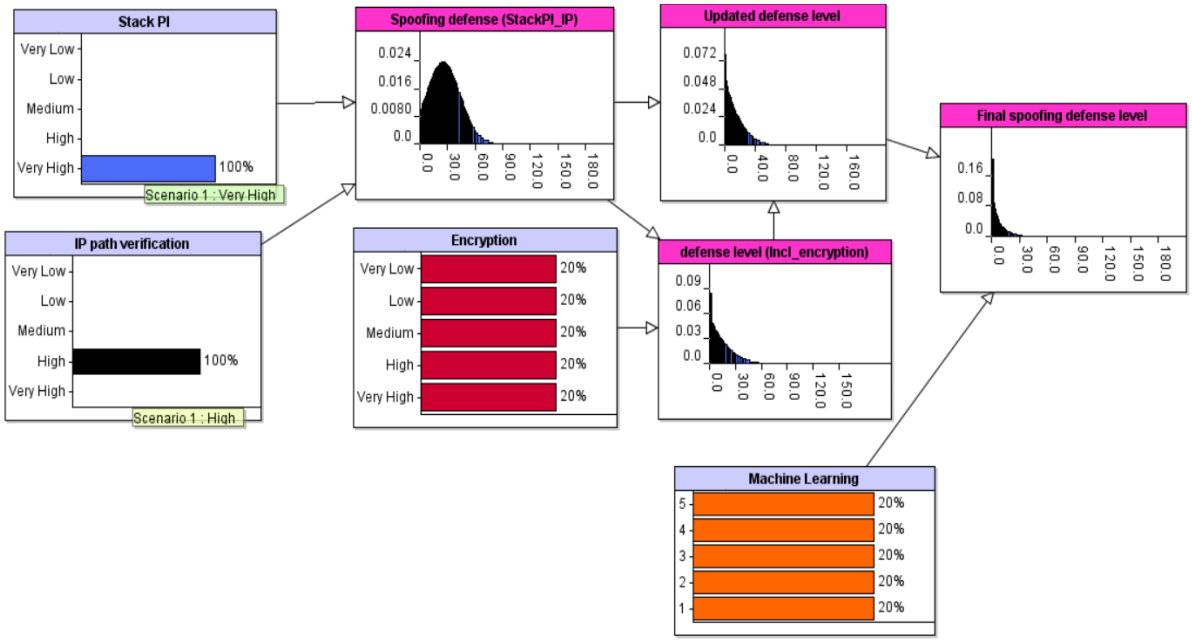

Figure 5.6: Scenario 1

Assuming a scenario where a financial service provider has a very effective implementation of stackPI and high IP path authentication the risk level is at a mean of 27.28; after implementing encryption, the mean drops to 19.11 and an updated mean of 8.18. The introduction of machine learning reduces this mean to 6.86.

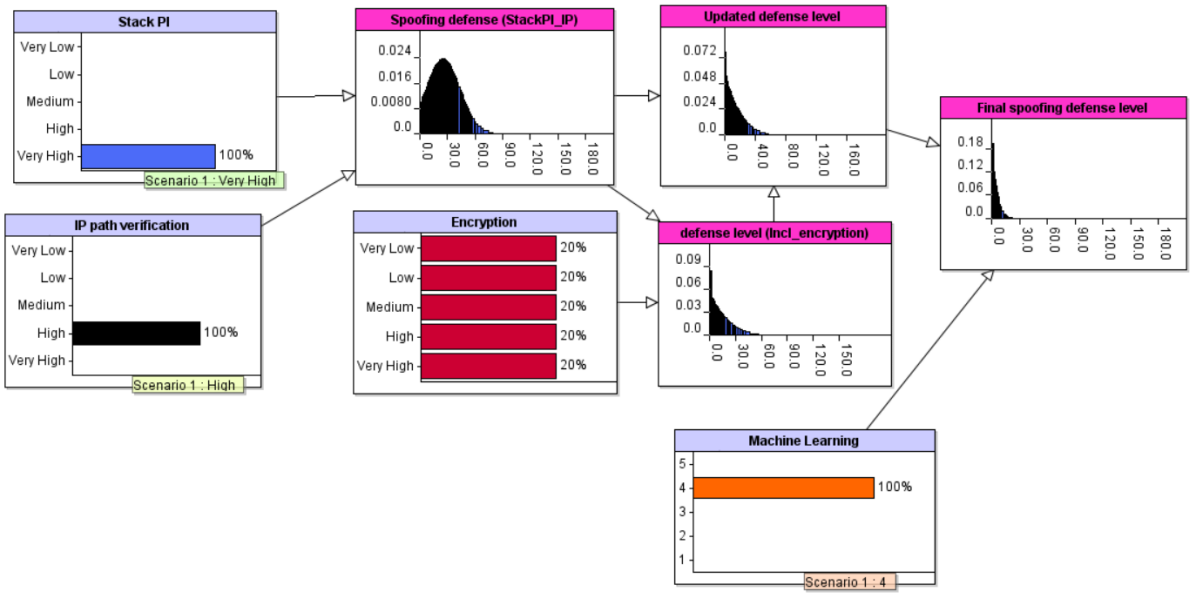

Figure 5.7: Scenario 2

If based on the above scenario the financial service provider decides to improve the efficiency of machine learning the final defense risk level significantly reduces to 1.39. Further, as depicted in figure 3.7, the mean keeps reducing with integration of another technique, and This clearly shows that an integration of these methodologies perform better than those that are standalone.

5.4 Sensitivity Analysis

Sensitivity analysis is important in understanding the relationship between variables and the impact that independent variables have on the dependent variables.

The interest in research was in the final defiance level; and the impact that the various antispoofing defense approaches have both as individual approaches and as a hybrid.

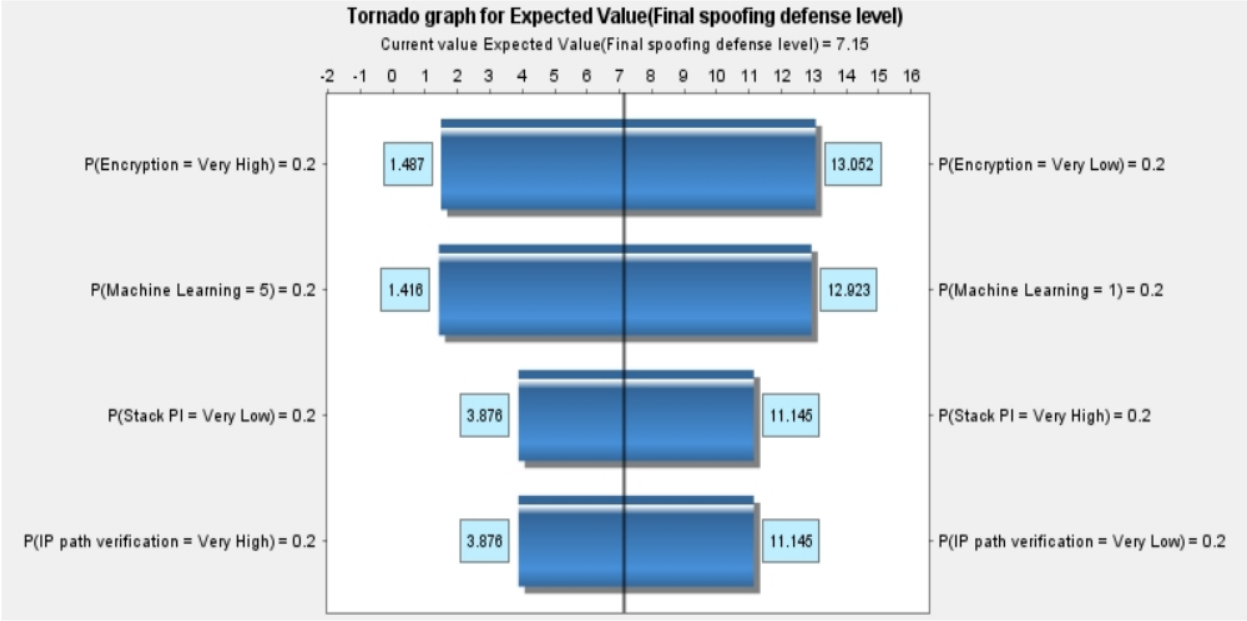

Figure 5.8: Tornado graph for final spoofing defense level

From figure 5.8, , it is clear that encryption has the greatest impact on the final defense against spoofing attacks followed by machine learning, stackPI and IP path verification. This goes to strengthen the assumption that the implementation of more than one approach effectively has the potential to cumulatively increase the defense against spoofing attacks. Individually the approaches have their strengths and weaknesses and provide to their own extent defense against spoofing attacks, a hybrid approach however combines this strengths and by extension overshadow some of the weaknesses. This ensures that the overall framework generally achieves more than what an individual approach would.

5.5 Summary of integration

A synergy between machine learning and filtering methods, and encryption provides an optimum defense mechanism against spoofing attacks. Once an IP and subsequent subnet is detected to have initiated a spoofing attack and fails to authenticate it is blacklisted and all packets from this source are dropped.

CHAPTER 6

6.0 CONCLUSIONS AND RECOMMENDATIONS

6.1 Introduction

This chapter presents the key study findings, conclusions, recommendations and suggested areas of further research.

This research focused on the integration of three methodologies, Stack Pi, Encryption informed by Machine learning as defense mechanisms for spoofing attacks. The proposed framework presented an integrated approach, that demonstrated the different methodologies complementing each other and presented several advantages including; ensuring high speed filtering of spoofed packet, enhancement in packet transmission, and once secure transmission is established no role of participating router in filtering process. This reduced on the amount of resources utilized during defense.

Implementing encryption and authentication will reduce spoofing threats this was further enhanced by ensuring that the proper authentication measures are in place and carried out over a secure (encrypted) channel. With the help of cryptosystem the speed of detection and prevention of IP spoofed packet was enhanced.

StackPi-IP filter further enabled the framework to possess traceback abilities where the victim can consult its database to generate a list of IP addresses that correspond to the packet's StackPi mark. Once this list is compiled, the victim can determine the paths by simply executing *traceroutes* to the addresses on the list. This reduce the space of potential attackers and allowed the victim's administrator to cull the true attack path using external knowledge and intuition. Machine learning could also be used to enhance traceroute capabilities by inferring information depending on past experiences.

Machine learning was incorporated in this framework to address the short comings of StackPi-IP filtering method and thereby increasing its efficiency. In machine learning this was done via three approaches: by inferring StackPi markings of previously unseen IP addresses, by inferring multiple StackPi markings in case of multi-path or short path and by inferring StackPi marking change caused by route change.

6.2 Recommendations and future Research

Further Research should explore the scope of integrated solutions as a defense mechanism in spoofing attacks and any other security issues that threaten information systems. Other forms of Artificial Intelligence such as particle swarm optimization (PSO) and genetic algorithms (GA) can be explored in the fight against spoofing attacks.

REFERENCES

Abrazhevich, D. (2001). Electronic payment systems: issues of user acceptance. 354-360.

Anthony, J., Pavel, L., Fabio, R., Tygar, D., & Blaine, N. (2014). *Machine learning methods for computer security.* Germany: Dagstuhi Publishing.

Bacard, A. (1995). *The computer privacy handbook.* Berkeley, . (1995). (, CA:).: Peachpit Press.

Bangar, P. C., Mulani, J.A, Ekad, A.B, Ganjewar, P.D, & Shinde, P. (2012). Study of IP-Spoofed Distributed DoS Attacks Using Hashed Encryption Scheme. *International Journal of Computer Science, Information Technology and Management*, 1-2.

Barreno, M., Nelson, B., & Joseph, A.D. (2010). The security of machine learning. *IEET*, 121–148.

Beimel, A., Kasiviswanathan, S. P., & Nissim, K. (2012). Bounds on the sample complexity for private learning and private data release. *In Theory of Cryptography Conference (TCC)*, (pp. 437–454.).

Bhaya, W., & Alasady, S. (2012). Prevention of Spoofing Attacks in the Infrastructure Wireless Networks. *Journal of Computer Science, 8* (10), 1769-1779.

Biggio, B., Momin, Z., Fumera, Marcialis, & Roli. (2010). Security evaluation of biometric authentication systems under real spoofing attacks. *IET Biometrics*, 11–24.

Bruschi, D., Ornaghi, A., & Rosti, E. (2003). S-ARP; A secure address resolution protocol. *19th Annual Computer Security Application Conference (ACSAC).* Milan: Universita` degli Studi di Milano.

CERT. (2006). *CERT/CC Statistics.* Retrieved from http://www.cert.org/stats/cert stats.html

Chau, P., & Poon, S. (2003). Octopus: an e-cash payment system success story. *Communications of the ACM*, 129-133.

Das, V., Janahanlal, S, & Yogesh, C. . (2011). Computer Networks and Information Technologies:. *Second International Conference on Advances in Communication, Network, and Computing, CNC 2011, Bangalore, India, March 10-11, 2011 proceedings.* Bangalore: Springer Science.

Douglas, E. (2006). *Internetworking with TCP/IP:Principles, Protocols, and Architecture.* Pearson.

Felten, E., Balfanz, D., Dean, D., & Wallach, D.S. (1997). *Web Spoofing: An Internet Con Game.* New Jersey: Princeton University.

Felten, E., Balfanz, D., Dean, D., & Wallach, D.S. (2013). *Technical Report 540-96 on Web Spoofing.* Department of Computer Science. New Jersey: Princeton University.

Ferguson, P., & Senie, D. (1998). Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing. *IEFT*, 1-10.

Gavaskar, S., & Ramaraj, E. (2011). A Compressed Anti IP Spoofing Mechanism using Cryptography. *International Journal of Computer Technology and Applications, 2*(2), 242-247.

Gupta, V., & Kavyashree, H. (2013). Comparative Study of IP Address Spoofing: Attacks and Their Defense Mechanism. *International Journal of Innovative Research and Studies, 2*(5), 2319-9725.

Haney, J. (2006). The use of cryptography to create data file security: with the Rijndael cipher block. *Journal of Computing Sciences in College, 21*(3), 30-39.

Haque, A., Tarofder, A.K, Rahman, S., & Raquib, M.A. (2009). Electronic transaction of internet banking and its perception of Malaysian online customers. *African Journal of Business Management, 3*(6), 248-259.

Harris, H., Guru, B.K, & Avvari, M.V. (2011). Evidence of Firms' Perceptions toward Electronic Payment Systems (EPS) in Malaysia. *International Journal of Business and Information*.

Hataiseree, R., & Banchuen, W. (2010). *The Effects of E-payment Instruments on Cash Usage: Thailand's Recent Evidence and Policy Implications.* Thailand: Payment Systems Department.

Henry, K. (2000). *Getting started with PGP. Crossroads: The ACM magazine for students.* Retrieved from http://dx.doi.org/10.1145/345107.345119.

Jarvenpaa, S., Tractinsky, N., & Vitale, M. (2000). Consumer trust in an Internet store. *Information Technology and Management, 1*(1), 45-71.

Joseph, A. D., Laskov, P., Roli, F., Tygar, D., & Nelson, B. (2012). *Machine Learning Methods for Computer Security.* Utah- Salt lake city: Dagstuhl Perspectives Workshop 12371.

Kandula, S., Katabi, D., Jacob, M., & Berger, A. (2005). Surviving Organized DDoS Attacks That Mimic Flash Crowds. *2nd Symposium on Networked Systems Design and Implementation (NSDI)* (pp. 287-300). Cambridge: MIT press.

Keizer, G. (2006, November 9). Fake site insist Microsoft Bought Firefox. *Information week.*

Kloft, M., & Laskov, P . (2010). Online anomaly detection under adversarial impact. *International Conference on AI and Statistics (AISTATS)* (pp. 405-412). Sardinia: JMLR: W&CP 9.

Kloft, M., & Pavel L, P. (2012). Security analysis of online centroid anomaly detection. *Journal of Machine Learning Research*, 3133–3176.

Kniberg, H. (2002). What makes a micropayment solution succeed? *Masters Thesis*. Stockholm: Kungliga Tekniska Högskolan (KHT).

Krüger, T., Gehl, C., Rieck, K., & Laskov, P. (2010). A self-healing web application firewall. *Symposium on Applied Computing (SAC),*, 1846–1853.

Lantz, B. (2013). *Machine Learning with R. 32 Lincoln Road.* Olton: Packt Publishing Ltd.

Lee, H., & Park, K. (2001). On the effectiveness of probabilistic packet marking for IP traceback under denial of service attack. *IEEE Infocomm 2001*. Indianna: Purdue University.

Li, J., Wang, J.M.M., Reiher, P., & Zhang, L. . (2002). Save: Source address validity enforcement protocol. *IEEE INFOCOM 2002*, (pp. 1557-1566). New York.

Lim, B., Lee, H., & Kurnia, S. . (2006). *Why did an electronic payment system fail?* Retrieved from A case study from the system provider's perspective: www.collecter2006.unisa.edu.au/ Paper%2011%20Benjamin%20Lim.pdf.

Linta, S, & Khan, R. (2013). *Today's Impact on Communication System by IP Spoofing and Its Detection and Prevention.* Santa Cruz: GRIN Verlag.

Marsland, S. (2011). *Machine Learning: An Algorithmic Perspective*. Florida, . (2011).:: CRC Press.

Meng, Y., & Kwok, L. (2013). *Enhancing false alarm reduction using pool-based active learning in network intrusion detection.* Lanzhou: Springer.

Messmer, E. (2007, January 25). Credit Card Industry Struggles to Enforce Security Standard. *Network World*.

Minho, S., & Jun, X. (2002). IP traceback-based intelligent packet filtering: A novel technique for defending against internet DDoS attacks. *IEEE ICNP* (pp. 1092-1648). Atlanta: Georgia Institute of Technology.

Minsky, H. (2010). *Investigating Computer Related Crime.* Florida: CRC Press.

Mohri, M., Rostamizadeh, A., & Talwalkar, A. (2012). *Foundations of Machine Learning.* Cambridge, Massachusetts: MIT Press.

Morein, G., Stavrou, A., Cook, D.L., Keromytis, A.D., & Misra, V. (2003). Using graphic turing tests to counter automated ddos attacks against web servers. *10th ACM International Conference on Computer and Communication.*

Moyle, E. (2007). *100 Million Notifications of Data Breaches in US.* Retrieved from www.TechNewsWorld.com

Nielsen, J. (1999, March 7). *Communicating trustworthiness in Web design.* Retrieved from Trust or bust: www.useit.com/alterbox/990307.html.

Oversight, P. S. (2012). *Summers. B.* London: Central Banking Publication Ltd.

Pastore, M. (2000, January 3). *Online consumer spending growth slowing.* Retrieved from Clickz Marketing news and expert advice: http://cyberatlas.internet.com/markets/retailing/article/0,,6061_271961,00.html.

Peng, T., Joshi, J., & Tipper, D. (2006). Survey of Network-based Defense Mechanisms Countering the DoS and DDoS Problems. *ACM Computing Surveys (CSUR), 39*(1).

Perrig, A., Song, D., & Yaar, A. (2002). *StackPi: A New Defense Mechanism against IP Spoofing and DDoS Attacks. School of Computer Science.* Pittsburgh: Carnegie Mellon University.

Ranjan.R, Ahmad, K., & Shekhar,J. (2010). IP spoof prevented technique to prevent IP spoofed attack. *VSRD Technical and Non-Technical Journal, 1*(3), 173-177.

Rekhter, Y., & Li, T. . (1995). A Border Gateway Protocol 4 (BGP-4). *IEFT RFC 1771*, 1-104.

Rieck, K., Trinius, P., Willems, C., & Holz, T. (2011). Automatic analysis of malware behavior using machine learning. *Journal of Computer Security, 19*(4), 639–668.

Sammut, C., & Webb, G. I. (2011). *Encyclopedia of Machine Learning.* Melbourne: Springer Science and Business Media.

Savage, S., Wetherall, D., Karlin, A., & Anderson, T. (2000). Practical network support for IP traceback. *2000 ACM SIGCOMM Conference.* Seattle: University of Washington.

Schneier, B. (2011). *Caller ID spoofing*. Retrieved from www.schneier.com.

Sevgi, Ö., Gayani, B., & Ray, H. (2010). Facilitating the adoption of e-payment systems: theoretical constructs and empirical analysis. *Journal of Enterprise Information Management, 23*(3), 305-325.

Shafinah, K., & Ikram, M. (2011). File Security based on Pretty Good Privacy (PGP) Concept. *Computer and Information Science, 4*(4), 10-28.

Shyamaladevi, V., & Wahidabanu, R.S.D. (2008). Analyze and Determine the IP Spoofing Attacks Using Stackpath Identification Marking and Filtering Mechanism. *IJCSNS International Journal of Computer Science and Network Security, 8*(10), 339.

Sio-Iong, A. (2010). *Machine Learning and Systems Engineering.* New York: Springer Science and Business Media.

Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. *IEEE Symposium on Security and Privacy,* 305–316.

Song, D. (2002). *StackPi: A New Defense Mechanism against IP Spoofing and DDoS Attacks.* Pittsburgh: Carnegie Mellon University.

Soon, L. (2012). *IP Spoofing Defense: An Introduction.* Selangor: Universiti Putra Malaysia.

Stallings, W. (2002). *Network security essentials: application and standards.* New Jersey: Prentice-Hall.

Stallings, W. (2006). *Cryptography and network security principles and practice.* Retrieved from ftp://shell.shore.net/members/w/s/ws/S

Sumanjeet. (2009). *Merchant risk, high costs, and lack of affordability.*

Summers, B. (2012). *Payment Systems: Design Governance and Oversight.* London, .: Central Banking Publication Ltd.

Upadhyay, V., & Kumar, R. (2011). Detecting and preventing IP spoofed attack by hashed encryption. *Journal of Enterprise Computing and Business Systems, 1*(2).

Vartanian, T., Ledig, R.H., & Ansell, D.L. (2004). Role and Security of Payment Systems in an Electronic Age. *Current Developments in Monetary and Financial Law* (pp. 1-18). IMF Institute.

Wyld, D., Wozniak, M., Chaki, N., Meghanathan, N., & Nagamalai., C. (2011). *Trends in Network and Communications.* Chennai: Springer Science and Business Media.

Yaar, A. (2002). StackPi: A New Defense Mechanism against IP Spoofing and DDoS Attacks. *Reasearch Show Case*, 1-24.

Zargar, S. T., Joshi, J., & Tipper, D. . (2013). A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE communications surveys and tutorials*, 1-24.

Zhang, F. (2012). *Multifaceted defense against distributed denial of service attacks: prevention, detection, mitigation.* Chalmers: University of technology Gothenburg.

Zimmerman, P. (1995). *PGP Source Code Internals.* Colarado: MIT Press.

APPENDICES

Appendix I: Letter of Introduction

January 2014,

Dear Respondent,

RE: REQUEST FOR RESEARCH DATA

I am a postgraduate student at Jomo Kenyatta University of Agriculture and Technology, pursuing a course leading to a Masters Degree of Science in Computer Systems. In partial fulfillment of the requirements of the stated degree course, I am conducting a Research Project entitled **"STACK PATH IDENTIFICATION AND ENCRYPTION ADOPTED AS SPOOFING DEFENSE MECHANISM TO ASSIST IN THE ADOPTION OF ELECTRONIC PAYMENT SYSTEMS"**

To achieve this, you have been selected in this organization to participate in this study. I kindly request you to fill the attached semi structured questionnaire so as to generate data required for this study. This information will be used purely for academic purposes and your name will not be mentioned in the report. Findings of the study, shall upon request, be availed to you.

Your assistance and cooperation will be highly appreciated.

Yours truly

Anne Kaluvu

STUDENT

Appendix II: Technical Respondents Questionnaire

Respondent's questionnaire on **Stack Path Identification and Encryption Adopted as Spoofing Defense Mechanism to assist on the adoption of Electronic Payment Systems**

SECTION A

1. Name (Optional) …….

2. Please state your gender

   ☐ Male ☐ Female

3. Kindly state your position in the company…….

4. Kindly select your age group.

   25 and below ☐

   26 – 35 ☐

   36 – 55 ☐

   Over 55 ☐

5. Please state your level of education

Postgraduate ☐

Graduate ☐

Middle level college ☐

Any other (please specify) ……

6. Please indicate your responsibility in the organization.

……

……

……..

SECTION B

Part I: The effects of spoofing attacks on the adoption of online EPS systems.

1. Do you use online EPS Systems?

Yes ☐ No ☐

1b). Which online EPS system do you use in your organization?

i. _____

ii. _____

iii. _____

1c). Please rate the following advantages of adopting an EPS system

Advantages of adopting EPS	**Most Favored (5)**	**Favored (4)**	**Neutral (3)**	**Less Favored (2)**	**Least Favored (1)**
Increased speed					
Increased convenience					
More efficient					
Reduced cost					
Increased customer base					

Part II: The awareness level of spoofing attacks on online payment systems.

1. Are you aware of spoofing attacks on online EPS Systems?

Yes ☐ No ☐

2. Have you experienced spoofing attacks on your online EPS systems?

Yes ☐ No ☐

2b). If yes, which forms of spoofing attacks have you encountered?

Forms of spoofing attacks	**Most Encountered (5)**	**Encountered (4)**	**Neutral (3)**	**Less Encountered (2)**	**Least Encountered (1)**
Web spoofing					
URL spoofing					
DNS spoofing					
IP spoofing					
Email spoofing					
Mac spoofing					
TCP spoofing					

3. Do spoofing attacks have a negative influence on the adoption of online EPS systems?

Yes ☐ No ☐

3b). If Yes above, how do spoofing attacks influence your adoption of online EPS systems?

Negative influences of	**st countered (5)**	**Encountered (4)**	**Neutral (3)**	**Less Encountered**	**Least Encountered**

spoofing attacks				**(2)**	**(1)**
Denial of services					
Corporate espionage and sabotage					
External invaders					
Lack of consumer confidence on systems					

Part III: The techniques that have been developed and applied to curb the presence of spoofing attacks.

1. Have you applied some techniques to curb spoofing attacks on your EPS Systems?

Yes ☐ No ☐

1b) If yes above, what techniques have been successful?

Techniques to curb spoofing attacks	**Most Successful (5)**	**Successful (4)**	**Neutral (3)**	**Less Successful (2)**	**Least Successful (1)**
Network ingress filtering					
Distributed packet filtering					
Cryptography (Encryption)					
ICMP message for traceback					
Pushback					
Hop-count filtering					
IP traceback					
Path identification					
Cisco NetFlow					
Secure Quality-of-					

Service					
Stack Path Identification					

2. What are some of the weaknesses experienced in the application of these techniques?

i. _____

ii. _____

iii. _____

Part IV: How a combination of techniques performs better in comparison to individual techniques.

1. Have you applied any combination of the above techniques?

Yes ☐ No ☐

1b). If yes above, what combination(s) of techniques did you apply?

i. _____

ii. _____

iii. _____

2. What is the success rate of this combination(s)?

Success factors	Most Successful (5)	Successful (4)	Neutral (3)	Less Successful (2)	Least Successful (1)
Improved efficiency in eradication of spoofing attacks					
Less time consumed between identification and curbing process					
Better indicators for the spoofing source					

3. Please list some of the short comings of the above combinations you have experienced

i. _____

ii. _____

iii. _____

Part V: How a combination of Stack PI and Encryption can be used to improve the performance of prevention of spoofing attacks.

1. Have you used Stack PI and Encryption combination?

Yes ☐ No ☐

1b) If Yes, please rate the success of Stack PI and Encryption combination

Success factors	Most Successful (5)	Successful (4)	Neutral (3)	Less Successful (2)	Least Successful (1)
Improved efficiency in eradication of spoofing attacks					
Less time consumed between identification and curbing process					
Better indicators for the spoofing source					

1c) If No, above do you think Stack PI and Encryption would achieve the following? Please rate.

Possible success factors of Stack PI and Encryption combination	Most Successful (5)	Successful (4)	Neutral (3)	Less Successful (2)	Least Successful (1)
Improved efficiency in eradication of spoofing attacks					

Less time consumed between identification and curbing process					
Better indicators for the spoofing source					

Thanks for Participating!

Appendix III: Management Questionnaire

Respondent's questionnaire on **Stack Path Identification and Encryption Adopted as Spoofing Defense Mechanism to assist on the adoption of Electronic Payment Systems**

SECTION A

1. Name (Optional) …….
2. Please state your gender

   Male ☐ Female ☐
3. Kindly state your position in the company…….
4. Kindly select your age group.

   25 and below ☐

   26 – 35 ☐

   36 – 55 ☐

   Over 55 ☐
5. Please state your level of education

   Postgraduate ☐

   Graduate ☐

   Middle level college ☐

Any other (please specify) ……

6. Please indicate your responsibility in the organization.

……

……

……..

SECTION B

Part I: The effects of spoofing attacks on the adoption of online EPS systems.

1. Do you use online EPS Systems?

Yes ☐ No ☐

1b). Which online EPS system do you use in your organization?

i. _____

ii. _____

iii. _____

1c). Please rate the following strategic advantages of adopting an EPS system

Advantages of adopting EPS	**Most Favored (5)**	**Favored (4)**	**Neutral (3)**	**Less Favored (2)**	**Least Favored (1)**
Increased speed					
Increased					

convenience					
More efficient					
Reduced cost					
Increased customer base					

Part II: The awareness level of spoofing attacks on online payment systems.

1. From a management perspective are you aware of spoofing attacks on online EPS Systems?

   Yes ☐ No ☐

2. Have you received any reports on spoofing attacks on your online EPS systems?

   Yes ☐ No ☐

   2b). If yes, which forms of spoofing attacks have been reported for your attention?

Forms of spoofing attacks	**Most Encountered (5)**	**Encountered (4)**	**Neutral (3)**	**Less Encountered (2)**	**Least Encountered (1)**
Web spoofing					
URL spoofing					
DNS spoofing					
IP spoofing					
Email spoofing					
MAC spoofing					
TCP spoofing					

3. Do spoofing attacks influence your decisions of procuring online EPS systems?

Yes ☐ No ☐

3b). If Yes above, rate the following as some of the reasons for procurement of your online EPS systems.

Negative influences of spoofing attacks	st countered (5)	Encountered (4)	Neutral (3)	Less Encountered (2)	Least Encountered (1)
Denial of services					
Corporate espionage and sabotage					
External invaders					
Lack of consumer confidence on systems					

Part III: The techniques that have been developed and applied to curb the presence of spoofing attacks.

1. Have you procured any techniques to curb spoofing attacks on your EPS Systems?

   Yes ☐ No ☐

1b) If yes above, what were successfully procured?

Techniques to curb spoofing attacks	Most Successful (5)	Successful (4)	Neutral (3)	Less Successful (2)	Least Successful (1)
Network ingress filtering					
Distributed packet filtering					

Cryptography (Encryption)					
ICMP message for traceback					
Pushback					
Hop-count filtering					
IP traceback					
Path identification					
Cisco NetFlow					
Secure Quality-of-Service					
Stack Path Identification					

2. What are some of the weaknesses that the technical staff reported to have experienced during the application of these techniques?

i. _____

ii. _____

iii. _____

Part IV: How a combination of techniques performs better in comparison to individual techniques.

1. Has the technical staff suggested any of the above combination of techniques to be adopted?

Yes ☐ No ☐

1b). If yes above, what combination(s) of techniques were applied?

i. _____

ii. _____

iii. _____

2. What is the success rate of this combination(s)?

Success factors	Most Successful (5)	Successful (4)	Neutral (3)	Less Successful (2)	Least Successful (1)
Improved efficiency in eradication of spoofing attacks					
Less time consumed between identification and curbing process					
Better indicators for the spoofing source					

3. Please list some of the short comings reported by the technical staff in relations to the above combinations that have been experienced

i. _____

ii. _____

iii. _____

Part V: How a combination of Stack PI and Encryption can be used to improve the performance of prevention of spoofing attacks.

1. Would you use Stack PI and Encryption combination if it was suggested to you?

Yes ☐ No ☐

Thanks for Participating!