Security Challenges and Solutions for E-Business

Anne James[1], Waleed Bulajoul[1], Yahaya Shehu[1], Yinsheng Li[2] and Godwin Obande[1]

1. Faculty of Engineering, Environment and Computing, Coventry University, United Kingdom
2. Software School of Fudan University, Fudan University, Shanghai, China

csx118@coventry.ac.uk (Anne James)
bulajouw@uni.coventry.ac.uk (Waleed Bulajoul)
shehuy2@uni.coventry.ac.uk (Yahaya Shehu)
liys@fudan.edu.cn (Yinsheng Li)
obandeg@uni.coventry.ac.uk (Godwin Obande)

Abstract

The advantages of economic growth and increasing ease of operation afforded by e-business and e-commerce developments are unfortunately matched by growth in cyberattacks. This paper outlines the common attacks faced by e-business and describes the defenses that can be used against them. It also reviews the development of newer security defense methods. These are: (1) biometrics for authentication; parallel processing to increase power and speed of defenses; (2) data mining and machine learning to identify attacks; (3) peer-to-peer security using blockchains; (4) enterprise security modelling and security as a service; and (5) user education and engagement. The review finds overall that one of the most prevalent dangers is social engineering in the form of phishing attacks. Recommended counteractions include education and training, and the development of new machine learning and data sharing approaches so that attacks can be quickly discovered and mitigated.

Keywords

E-business security; e-commerce security; security solutions

1. Introduction

Electronic business (e-business) is the use of the internet, intranet, extranet or other networks to support business processes. It includes various activities such as buying and selling electronically, electronic procurement, electronic distribution, online customer service, electronic marketing, secure transactions, automation of processes, and electronic collaboration. E-commerce on the other hand generally refers to the buying and selling, marketing and servicing, and delivery and payment of products, services and information over the internet, although other electronic mediums can be used. It is part of e-business.

The advantages of economic growth and increasing ease of operation afforded by e-business and e-commerce developments are unfortunately matched by growth in cyberattacks [1, 2]. The aim of these attacks is usually financial gain. Sadly the Anti Phishing Working Group (APWG) recorded more phishing in 2016 than in any year since it began monitoring in 2004 [1] with a 65% increase on 2015 figures. According to the latest APWG Activity Report, over 80% of phishing attacks target retail services, financial institutions, Internet Service Provider (ISP), or payment services. These attacks are normally not mitigated quickly, with average uptime of 29h and 51min in 2014 [3]. Thus the fake interfaces have plenty of time to trap victims before they are removed.

The Symantec 2016 Internet Threat Report [2] highlighted that over the previous year there was a 125% increase in zero-day attacks where vulnerabilities are exploited before the software owners are aware of them. It also reported that 78% of websites have unpatched vulnerabilities and that there is a rise of ransomware attacks where attackers encrypt or lock owner's data and do not release it until a ransom is paid. A recent example of a ransom attack is the WannaCry malware which affected many organization around the world in 2017. The report also noted a rise in attacks against small business (those with 250 or fewer employees) although there was a decrease in the number of small businesses attacked, evidencing more targeted attack campaigns. Indeed increased by 55% are spear phishing attacks. In these attacks individuals or organizations are targeted after the attacker has obtained information about them and then uses that information to gain trust. The report also stated that the Internet of Things (IoT) presents greater risks as the technology develops and becomes more widespread.

There have been significant technological advancements in developing tools to prevent attacks on electronic communication over the internet. Examples include tools which alert users of potentially fraudulent emails and websites but, as also extensively reported in literature, these tools are not entirely reliable in protecting users against attacks [4, 5]. Security experts and attackers compete against each other. Experts, with the help of developers, continue to develop software to prevent attacks while attackers are constantly learning new techniques and changing tactics to make attacks more successful. Furthermore the "human" is often the weakest link in information security chain rendering technical innovations powerless when successfully attacked through social engineering [6].

In the following sections of this paper, a review is provided of security in e-business, concentrating on the e-commerce area as this area is the most targeted and vulnerable. In section 2, current security threats are reviewed. Section 3 looks at current solutions, while section 4 discusses new developing approaches. Section 5 offers a conclusion to the paper.

2. Current security threats in E-commerce

Many of the current security threats are especially damaging in the e-commerce side of e-business. This is the area where exchanges of money for goods or services occur and thus are of particular interest to users with bad intent for financial gain. There are a number of common vulnerabilities. As early as 2001 a survey by Udo [7] showed that the major hurdles to using e-commerce were privacy and security concerns. In 2014, Hartono et al. [8] found that buyer concern about website security is still a critical issue when it comes to maximizing the potential for electronic commerce transactions. Furthermore in 2016, Jotwani and Dutta highlighted e-commerce security threats, emphasizing the importance of information security in the financial transactions of e-commerce [9]. Security threats in e-commerce can be divided into three main types: denial of service (DoS); spying attacks; and unauthorized access. Within these types there are many methods of attack and there are overlaps between the areas, with some methods being common to more than one type of threat. The following sections discuss these three main threats.

2.1 Denial of Service

A denial of service attack aims to make the target service overwhelmed with messages such that it is no longer able to execute satisfactorily, thus denying users access to the service. It is achieved by bombarding the service with requests usually generated automatically. IP Spoofing may be used to start a DoS attack. IP spoofing involves changing the source address of a data packet so that it looks like it has come from a recognized and trusted source. Since the server logs will already contain the spoof address, it is difficult to find the source of the attack. The denial of service attack these days is usually a distributed attack called a Distributed Denial of Service (DDoS) attack where requests are sent from many sites, often as a result of

participating attack sites being compromised after being infected with malicious software (see description of Trojan attacks in section 2.2). The participating sites act maliciously without the owner's knowledge.

Another type of DoS attack is to infect the target with a virus such that it is no longer able to function. A computer virus is a malware program that replicates itself and spreads through a network and might be set up to deliberately corrupt or delete data. The virus is usually spread via attachments in emails or via downloads. When the user opens the file, the virus will be activated. It may then continue to spread its code into other programs and files stored on the victim computer. A computer worm operates similarly to a virus but does not carry a payload to cause damage to the victim system. A worm can however still cause problems by taking up valuable bandwidth and thus denying service.

2.2 Unauthorized Access

Unauthorized access means accessing a system without permission. There are various ways in which this might be achieved. One method is through back doors. A back door is an access channel to a site that bypasses normal authentication methods. They are used by developers to enable quick and easy access during development and should be removed before the software is released. Any which remain are a threat to security as attackers often attempt to access the site through the server side. Back doors are sometimes in place for legitimate reasons such as troubleshooting or restoring user passwords but they are not recommended since they become an area of vulnerability regarding security. Open ports are another vulnerability. A port scanner might be used to find open serviced ports through which a DDoS attack can be launched. Port scanning is also a method used legitimately by administrators to check security of their systems. At a higher level, a ping sweep can be used to find which IP addresses map to live hosts. A live host sends an echo-reply and can then be probed further by an attacker.

The attacker may obtain credentials by social engineering which refers to persuading or tricking humans into passing on their credentials. This can be achieved by person-to person contact, often over the phone with the attacker posing as a legitimate agent for an entity with which the victim has a relationship, or by machine-to-person contact through phishing. Phishing attacks are used to illegitimately gain credentials by presenting what seems to be a trusted and recognizable system interface to the user but it is actually false and linked to the attacker's domain. The legitimate user thinks they are accessing the real system but unfortunately they are not. Instead the user's credentials get passed to the attacker's site while the user receives a benign message generated by the attacker so that suspicions are not aroused. By this time the attacker has the user credentials and can access the system.

Often social engineering is used to launch a Trojan horse or Trojan attack where the victim is duped into opening an email attachment or downloading some software. The Trojan attack takes the form of a malicious computer program which creates a back door to the affected computer. It does this by connecting to a controller which can then have unauthorized access to the victim machine enabling the attacker to access everything in the affected computer, modify or delete data and upload further software. Personal information such as banking information, passwords, or personal identity (IP address) can be stolen. The controller might gradually gain control of a number of machines, collectively termed a Botnet, which it can use to create a DDoS attack (see section 2.1).

Another category of attack worth mentioning is that of stealth attacks [10, 11]. A stealth attack as one that remains undetected by the client computer. Stealth attackers targeting a victim may move patiently through computer networks, taking days, weeks or months to accomplish their objectives, in order to avoid detection. As networks scale up in size and speed, monitoring for such attack attempts is increasingly a challenge [12]. Other methods of unauthorized access include brute force attacks where the attacker gains

access by trial and error, continually attempting to guess the password. A predeveloped list of possible passwords or automated software may be used to generate a large number of consecutive guesses.

2.3 Spying Attacks

Spying attacks include sniffing. Sniffers are applications or devices that can read, monitor, and capture network data exchanges and read network packets. Without strong encryption, data can be read by sniffers as they traverse the network. Having access to the data gives attackers the ability to gain sensitive information which can be used for criminal offences. The man-in-the-middle (MITM) attack is where an attacker intercepts a conversation between two parties and relays messages between the parties impersonating each of them. The attacker thus gains access to information that the two parties were exchanging and may also change messages or send false messages. The MITM attack could be used to send a Trojan horse (see section 2.2).

Another type of spying attack is key logging. A key logger is a hardware device or small program that monitors each keystroke a user types on a specific computer's keyboard. As a hardware device, a key logger is a small battery-sized plug that serves as a connector between the user's keyboard and computer. As the user types, the device collects each keystroke and saves it as text in its own miniature hard drive. At a later point in time, the person who installed the key logger must return and physically remove the device in order to access the harvested information. A key logger program, on the other hand, does not require physical access to the user's computer. It can be downloaded on purpose by someone who wants to monitor activity on a particular computer or it can be downloaded unwittingly as spyware and executed as part of a rootkit (software designed to enable access to areas of system software that would not otherwise be allowed) or through a remote administration Trojan (RAT) (see section 2.2). A key logger program typically consists of two files that get installed in the same directory: a dynamic link library (DLL) file (which does all the recording) and an executable file that installs the DLL file and triggers it to work. The key logger program records each keystroke the user types and uploads the information over the internet to the installer.

2.4 Summary of attacks and methods

Table 1 shows categories of attack and methods that are commonly used and which were discussed in the previous sections.

Table 1: Attacks and Methods

Category	Attack	Contributing Method
(Distributed) Denial of Service	Stops legitimate users being able to access the service or impairs performance of a service	Message Bombardment Botnet IP Spoofing Virus Worm
Spyware	Discovers sensitive information	Sniffer Man in the Middle Key logger
Unauthorized Access	Commits crimes like manipulating records for financial gain, carrying out unauthorized operations, placing viruses or malware	Social Engineering (including Phishing) Password cracking Back door Stealth Attack

3. Current security solutions

Generally, security can be defined as an organized framework consisting of concepts, beliefs, principles, policies, procedures, techniques, and measures that are required in order to protect the individual system assets as well as the system as a whole against any deliberate or accidental threat [13]. The AIC triangle (availability, integrity and confidentiality) is a model designed to guide the development of policies for information security in organizations (see Figure 1). Availability means ensuring that data needed is available at all times to those that need it. Integrity means ensuring that the data is correct and protected from unauthorized modification or unintended corruption. Confidentiality means that data stored on the computer must only be accessible to those with a right or need to see it. The AIC model is widely accepted in organizations and considered to be a cornerstone of security maintenance. Various methods can be used to support the AIC objectives. These include authentication, encryption, access control, firewalls, intrusion detection and prevention systems, message digest or checksum, honeypot, digital signature, and digital certificate. Table 2 shows the approaches used and how they relate to the AIC model.

Authentication is the process of proving the identity of the user or process to the receiving system. It is commonly implemented through names and passwords. Cards, tokens or biometrics may also be used but the standard legacy password offers a good balance of security versus convenience. Bonneau et al. [14] evaluated two decades of proposals to replace text passwords for general-purpose user authentication on the web using twenty-five usability, deployability, and security benefits that an ideal scheme might provide. The scope of proposals surveyed included password management software, federated login protocols, graphical password schemes, cognitive authentication schemes, one-time passwords, hardware tokens, phone-aided schemes and biometrics. The authors found that no known scheme came close to providing all desired benefits and none even retained the full set of benefits that legacy passwords already provide. They found a wide range of schemes from those offering minor security benefits beyond legacy passwords, to those offering significant security benefits in return for being more costly to deploy or more difficult to use.

Encryption is the converting of plain text to code or cypher-text in order to make it non-intelligible to anyone who views it without the necessary access rights. The cypher-text can only be decoded through the use of a key which only authorized users or processes should possess. Various methods of encryption can be used and research efforts continue to seek stronger solutions to combat the efforts of attackers [15]. Access control is the use of rules which state which users are allowed access to which objects. A principle is that users should only be able to access systems needed to carry out their assigned functions. Access control lists (ACL) are widely used in organizations and are usually role based.

Firewalls are hardware or software devices that protect a local network by monitoring and controlling the incoming and outgoing traffic based on predetermined security rules. They sit between a local network and the Internet. Intrusion detection and prevention systems (IDPS) work similarly but the latter have more functionality. They sit either on the local network (NIDPS) or host (HIDPS) and report, detect or protect systems. Intrusion detection and prevention systems (IDS, IPS or IDPS) monitor, detect, analyze and prevent intrusions. A system that protects important operating system files is an example of an HIDPS, while a system that analyzes incoming network traffic is an example of an NIDPS. IDPS can also be classified by detection approach. The detection method might be signature-based detection (recognizing bad patterns, such as malware) or anomaly-based detection (detecting deviations from a model of "good" traffic). Selecting the right response to an attack is an important part of intrusion detection. Responses include: generating a report or alarm; isolation; relocation; no punishment; service denial ; account locking;

ICMP messaging; remote logging ; IP address blocking; host shut down; disconnecting from the network; disabling attack port; or creating back up [16].

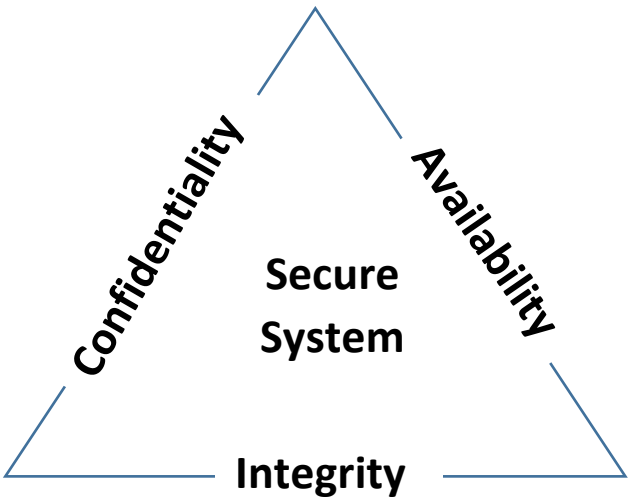

Figure 1: AIC Model

Message digests are secure one-way hash functions that take arbitrary-sized data and output a fixed-length hash value. Examples are the SHA algorithms [17]. They protect the integrity and of data since they can be used to check whether or not data has been modified. Any modification would produce a different hash value. Checksum is a similar method for protecting integrity. In this case a sum is made of the values of bytes in a piece of data to create a sum that can be checked. Any modification of the data would produce a different sum value. Honeypots are decoy systems intended to deflect attackers. They mimic the real systems and appear to have data attractive to attackers but they are isolated from the real site. They can be used to learn more about attacks and to keep the attackers away from the real system. Once an attacker is identified, they can be blocked from the real site.

Digital signature is part of Public Key Infrastructure (PKI). It manifests as a code which is attached to an electronically transmitted document to verify its contents and the sender's identity. In PKI, a user has a public key and a private key which are generated mathematically and verified by a certifying authority (CA). The digital signature is used to sign documents. A user encrypts the signed document with the private key and sends it together with the public key to the receiver. The receiver decodes the message with the sender's public key and is thus able to verify the sender. The document would not be possible to decrypt with the public key if it had not been encrypted with the private key. Digital signature therefore provides non-repudiation which means that the sender cannot deny having sent the document.

Digital certificates are also part of PKI. Digital certificates are electronic documents used to prove the ownership of a public key. Information about its owner's identity, as well as the digital signature of an entity that has verified that the certificate's contents, are included in the certificate. A potential sender can examine the certificate and check whether the signature is valid by using the verifying entity's public key. If the signature is valid, the sender will be reassured that they can use the certificate holder's public key to

securely send a message to the certificate holder. On receipt of the message the certificate holder uses their private key to decrypt the message.

Based on PKI and having evolved from Netscape's Secure Sockets Layer (SSL) protocol, Transport Layer Security (TLS) is the most-commonly used security technology for establishing an encrypted link between a web server and a browser. The terms SSL or SSL/TLS are used to refer to the same protocol. TLS provides privacy and data integrity between two communicating applications. It differs from the earlier SSL by providing more secure methods as part of its protocol. Key differences between SSL and TLS that make TLS a more secure and efficient protocol are message authentication, key generation and the supported cipher suites, with TLS supporting newer and more secure algorithms. A common higher-level protocol used in E-Commerce is HTTPS. It uses TLS to secure the communication as opposed to HTTP which does not. An important standard for a PKI to manage digital certificates and public-key encryption is X.509 [18]. The standard is a key part of the TLS protocol and includes formats for public key certificates, certificate revocation lists, attribute certificates, and a certification path validation algorithm.

Table 2: Approaches to Security Defense and the AIC Model

Method	**Purpose**	**AIC Model Relationship**
Authentication	Makes sure only legitimate users can access the system	Confidentiality Integrity
Encryption	Makes sure data cannot be read by unauthorized people	Confidentiality
Access Control	Makes sure users only access parts of the system they need	Confidentiality Integrity
Message digest or Checksum	Enables data to be checked for tampering	Integrity
Firewall	Prevents attackers from getting into the system	Confidentiality Integrity Availability
Intrusion Detection and Prevention Systems	Detects, analyses and prevents intrusions from outside and within a system	Confidentiality Integrity Availability
Anti-virus and anti-spyware	Detects, blocks and removes virus and spyware	Confidentiality Integrity Availability
Honeypot	Attracts attacks away from proper site and learns about them	Confidentiality Integrity Availability
PKI – digital signature and certificate	Ensures non-repudiation and that data can be sent securely over the internet using encryption	Confidentiality Integrity

4. New developments in security for e-business

In this section we discuss newer solutions to security defenses. Included are: biometrics for authentication; parallelism to increase power and speed of defenses; data mining and machine learning to identify attacks; peer-to-peer security using blockchains; enterprise security modelling and security as a service; and user education and engagement.

4.1 Biometrics for authentication

Biometrics [19] are becoming popular in user identification systems [20]. Biometrics are technologies for measuring and analyzing a person's physiological or behavioral characteristics. These characteristics are unique to individuals hence can be used to verify or identify a person. Arguably, biometrics provide a very convenient method of identification because a person always carries their biometrics with them and does not therefore need a card token or to remember a long password. However there are some issues with biometrics which hinder take-up [21, 22, 23] including accuracy and privacy concerns.

Biometric technologies for authentication are increasingly being adopted in e-business, particularly in developing nations. Nigeria is a country with an estimated population of over 167 million people [24]. A number of biometric initiatives have been introduced in recent years [25]. Banks were recently given directives to collate fingerprints of all their existing customers after which a unique Bank Verification Number (BVN) was issued to all customers. The reason of this was to enable checks and reduce fraud. All mobile phone operators in the country make it a policy that all their customers must register their SIM card (a registration that involves fingerprints) before they can have access to the network as directed by the Nigerian Communication Commission (NCC). The aim is to reduce fraud and criminal activity. In some states, ministries or agencies, fingerprints are used to uniquely identify genuine employees. The idea behind this is to check the rampant cases of ghost workers. These are workers who are on the pay roll but who will never be seen because they do not exist. However there have been issues with accuracy and confidence in some of these use cases. Coventry University UK is developing a system to increase confidence and performance in biometric authentication methods in partnership with a state government in Nigeria [26]. Nigeria is not the only country adopting widespread national use of biometrics. The Brazilian bank Bradesco uses a palm vein biometric system called Palm of Your Hand to provide secure log-in on its ATM machines. Clients can choose to use this biometric instead of their PINs. The national government of India is aiming to reduce benefit fraud with the roll out of a biometric identification database which will contain biometric details of all of its citizens. Nigeria, Brazil and India are nations which, in spite of rapid development, have many citizens still living in poverty. Some citizens do not have a birth certificate and in these cases biometrics can provide a good solution for proving identity. In the developed world we see fingerprints uses at Disney parks in the USA and thumb prints are commonly used across schools in the UK for lunch and refreshment purchase. Biometrics are also increasingly used in passports and national identity cards in many countries around the world. It is a technology that will be increasingly adopted. A standard biometric authentication procedure typically runs as follows. First a user registers their biometrics via a sensor, a template is generated and stored in a database. Subsequently to access the system, a user provides their biometrics again via a sensor, a new template is generated and compared to the previously stored template. If there is a match, access is allowed. If not, access is denied.

The fundamental objective of a biometric system is to recognize individuals accurately. This in turn implies that a biometric system must have low recognition error rates. FAR (False Acceptance Rate) and FRR (False Reject Rate) are used to quantify errors in verification systems. Many research efforts are devoted to creating systems which decrease false outcomes for varying modes of biometrics. A DET (Detection Error Tradeoff) curve is a plot which has FRR on the y-axis and the FAR on the x-axis. FAR and FRR are useful because the Equal Error Rate (EER) is deduced based on these two parameters. EER is a unique operating point where FAR=FRR. This summarizes the entire DET curve and can be interpreted to achieve the accuracy of detection by subtracting the EER value from 100. EER is commonly used as a measure to compare performance of different biometric systems.

There are many modes of biometrics that can be used for identification in authentication systems [27]. They include physical biometrics such as: fingerprints [28]; face recognition [29]; hand geometry [30]; iris recognition [31]; and palm vein identification [32]. Keystroke is an example of a behavioral biometric. Jain, Ross, and Prabhakar [33] identified seven factors for assessing the suitability of any trait for use in biometric authentication. These are: universality; uniqueness; permanence; measurability; performance; acceptability; and circumvention. Table 3 shows comparative performance in terms of EER of some popular biometric modalities.

Table 3: Performance Evaluation of Different Biometric Techniques

Biometrics	EER	Subjects	Comments	Research Source
Voice	≈10%	234	Recorded speech, gender characteristic aware algorithm. Better results obtained when gender specific features were used. ALBAYZIN and MOBIO speech corpora.	[34]
Keystroke	≈8%	300	Keystroke Biometrics Ongoing Competition (KBOC). Average of 15 best systems.	[35]
Face	≈5%	Over 2M	Average from a number of research works. Images and videos. Deep learning methods. Average score for images ≈2%. Average score for videos ≈8% Best result for images ≈1% (1.05) Best result for videos ≈3% [36].	[36, 37, 38, 39, 40, 41, 42]
Fingerprint	≈3%	Various	FVC2002 database. Average from a number of research works. Best result 0.44% [43].	[43, 44, 45, 46]
Hand Geometry	≈1.5%	≈1250 images	Based on two recent works. Best result achieved with genetic algorithm ≈0.9% [47].	[47, 48]
Iris	≈1.5%	Various	Reported EER from experiments on CASIA v3 Interval data set. Higher EER reported on CASIA v3 Lamp data set. Much lower EER reported on earlier data sets e.g., ≈0.001% EER on NIST Iris image base [49].	[49, 50, 51, 52, 53, 54]
Palm Vein	≈0.5%	Various	Average from a number of research works.	[55, 56, 57, 58, 59]

Since biometrics are unique to the person, they are more reliable in identifying individuals than passwords. However some biometrics change over time. Finger surfaces may wear or get damaged and irises may age and change [60]. Furthermore performance in terms of false results can be an issue. In case of the latter, multi-modal biometrics, where more than one method is used, could offer a more robust and better performing identification method [33]. There are privacy and accuracy concerns about collecting biometrics but, in spite of this, they are gradually gaining acceptance and increasingly being taken up by applications. Table 4 presents a comparison of some biometric modalities in terms of the seven comparison criteria introduced by [33] and based on the authors' viewpoint following research review.

Table 4: Comparison of Different Biometric Technologies based on the authors' viewpoint

Biometric	Universality	Uniqueness	Collectability	Permanence	Performance	Acceptability	Circumvention
Fingerprint	H	H	M	M	M	H	M
Face	H	M	H	M	L	H	H
Iris	H	H	H	H	H	M	L
Hand Geometry	H	M	H	L	H	H	M
Keystroke	L	L	M	L	L	L	M
Voice	M	H	M	L	L	H	H
Palm Vein	H	H	M	H	H	H	L

Following analysis of the various biometrics, the authors consider that palm vein technology offers great potential for use in biometric authentication in e-business. The liveness factor, namely that palm vein technology is based on thermal scanning and as such only works with a live palm, is very important as this avoids circumvention. It also seems to have higher acceptability than iris scanning, another technology with high performance. At Coventry University, UK, there is an on-going research project which is investigating the development of a BioPKI system which uses palm vein technology [61].

4.2 Parallelism to increase power and speed of defenses

Many studies on improving security have led to research into how parallel and multi-core technologies could benefit the efficiency and effectiveness of such systems.

Vasiliadis, Polychronakis, and Ioannidis [62] proposed a new model for a multi-parallel IDS architecture (MIDeA) for high-performance processing and stateful analysis of network traffic. Their solution offers parallelism at a subcomponent level, with processors within a host machine carrying out specialised tasks to improve scalability and running time. They showed that processing speeds can reach up to 5.2Gbps with zero packet loss in a multi-processor system. Jiang et al. [63] proposed a parallel design for a NIDS on a TILERAGX36 many-core processor. They explored data and pipeline parallelism and optimized the architecture by exploiting existing features of the processor to break the bottlenecks in the parallel design. The system was designed according to two strategies: first a hybrid parallel architecture was used, combining data and pipeline parallelism; and secondly a hybrid load-balancing scheme was used. They took advantage of the parallelism offered by combining data, pipeline parallelism and multiple cores, using both rule-set and flow space partitioning. They showed that processing speeds can handle and reach up to 7.2Gbps with 100-byte packets and 13.5 Gbps for 512-byte. Jamshed et al. [64] presented the Kargus system which exploits high processing parallelism by balancing the pattern matching workloads with multi-core

CPUs and heterogeneous GPUs. Kargus adapts its resource usage depending on the input rate, to save power. The research shows that Kargus handles up to 33 Gbps of normal traffic and achieves 9 to 10 Gbps even when all packets contain attack signatures.

Bul'ajoul, James and Pannu [65, 66] proposed an NIDPS solution for high-speed malicious traffic using QoS (Quality of Service) configuration and parallel technology. They designed a novel security architecture to increase the analytical, detection, and prevention performance of the NIDPS when facing high-speed traffic. Their study investigated the impact of parallelism in high-speed environments and how to achieve improvement through parallelization using industry-standard software systems and standard desktop processors. The study showed that security performance can be weak in the face of high-speed and high-load malicious traffic in terms of packet drops, outstanding packets and failing to detect/prevent unwanted traffic. Their solution used a novel QoS configuration in a multi-layer switch to organize and improve network traffic performance in order to reduce the number of packets dropped. The NIDPS used was Snort. Parallel techniques were used to increase processing speed performance. Results are shown in Figure 2 (processing time) and Figure 3 (processing speed).

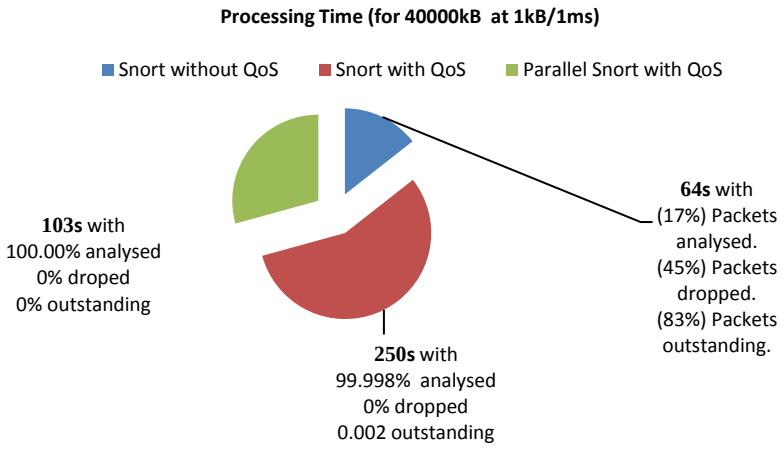

Figure 2: Parallel Snort NIDPS Processing Time for 40,000 1 kB packets sent at 1ms intervals

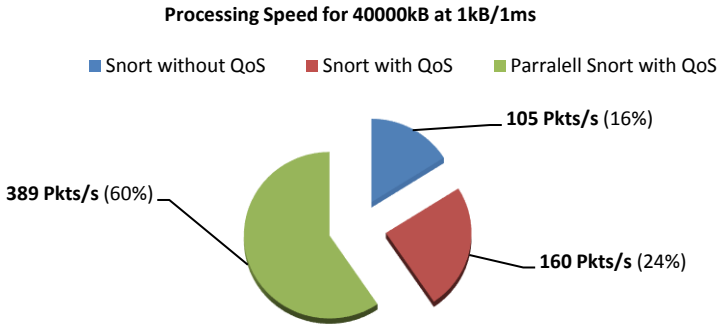

Figure 3: Parallel Snort NIDPS Processing Speed for 40,000 1 kB packets sent at 1ms intervals

The solution is based on configuring the network switch to shape traffic into queues, each queue having its own NIDPS, the complete set operating in parallel (see Figure 4). A differentiated services technology was used to modify, organize and control traffic based on the Differentiated Services Code Point (DSCP) value

which can offer more precise handling of traffic and classify each packet upon entry into the network interface, allowing for adjustments to be made for different traffic speed and loads. Incoming traffic was classified through a class map that which enabled packets to be processed as a group of bytes defined by policy and ACLs that were matched with DSCP values to allow each traffic group to be processed by separate queue.

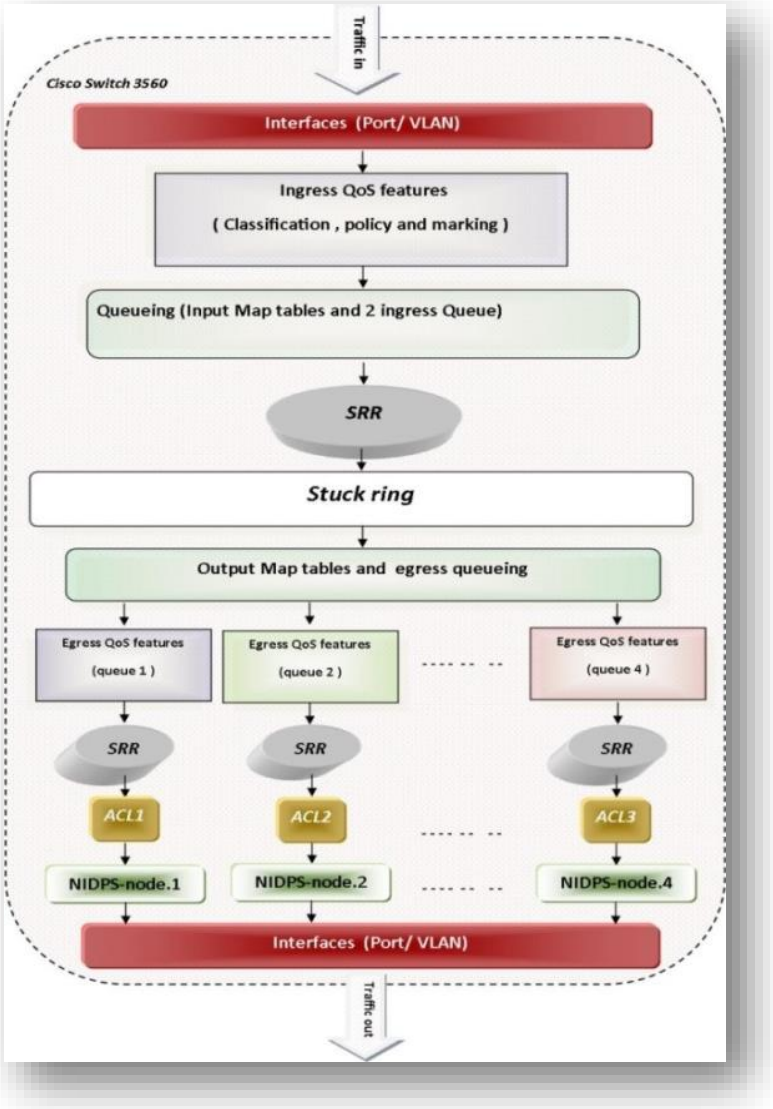

Figure 4: Novel architecture for NIDPS

The novel architecture was tested under different traffic speeds, types, and tasks. The experimental results show that the novel architecture along with the introduction of parallel technologies can increase the efficiency and effectiveness of security platforms and so improve overall security. By using 2x quad core machines connected to 2x 1 GB interfaces, the new architecture has been processed for up to 8Gbps traffic speed with 1kB packets. This solution is a more accessible way of receiving good results as it can be activated at a higher level, namely at the level of configuring the multi-core switch and replicating NIDPS on multi-core machines. Further improvements could be made if higher performance equipment were used. The solution can be extended to the idea of an elastic NIDPS which can grow as the traffic grows. This is

achieved by varying numbers of queues and NIDPS machines according to traffic. As traffic gets higher more NIDPS are engaged. The emergence of cloud computing provides the infrastructure for this type of solution. While traffic becomes heavier the number of NIDPS increases, while in the background, services search for anomalies to find the source of a possible malicious DDoS attack. Once sources are discovered, they can be blocked, traffic will decrease to normal levels, and the number of operational NIDPS can be decreased.

4.3 Data mining and machine learning to identify attacks

Data mining and machine learning offer good potential for increasing the power of intrusion detection and attack signature learning [67]. Stealth attacks, normally difficult to counteract, may be detected through the use of data mining techniques. Tran et al. [68] argue that due to the complex and dynamic nature of computer networks and hacking techniques, detecting malicious activities remains a challenging task for security experts. They proposed a novel machine learning algorithm which integrates an adaptive boosting technique and a semi parametric neural network to obtain good tradeoff between accuracy and generality. Feng et al. [69] proposed combining state vector machine and ant colony networks to mine network data for intrusion detection.

Finding anomalies in access or data logs through data mining can indicate an attack. However, since launching stealthy attacks is a sophisticated technique that may take place over months, it is theoretically necessary to keep a long history of activities in order to identify these attacks. Kalutarage et al. [12, 70] have proposed a technique based on anomaly detection and sampling in order to overcome this issue. Using peer and discord analysis, a monitoring algorithm based on Bayes probability is used to monitor network nodes at regular intervals and generate profiles with probabilities of whether an node is an attacker or not. A node showing an out-of-line profile can be further investigated. The approach maintains long-term estimates computed on sampled data rather than retaining event data for post-facto analysis, thus it significantly reduces the amount of data to handle and maintain, thereby increasing the chances of detecting the stealth attack.

4.4 Peer-to-peer security using blockchains

A new method that is gaining interest as a security defense is peer-to-peer security through blockchains [71].

> *"With blockchain, we can imagine a world in which contracts are embedded in digital code and stored in transparent, shared databases, where they are protected from deletion, tampering, and revision. In this world every agreement, every process, every task, and every payment would have a digital record and signature that could be identified, validated, stored, and shared. Intermediaries like lawyers, brokers, and bankers might no longer be necessary. Individuals, organizations, machines, and algorithms would freely transact and interact with one another with little friction. This is the immense potential of blockchain."*
>
> Lansiti M and Lakhani KR [72]

The blockchain approach has been used in transaction processing for Bitcoin, a decentralized crypto-currency, to provide financial data security on a distributed peer-to-peer platform [73]. No third parties are needed. This avoids issues of vulnerability of having all data in one place and also allows transactions to be cleared quickly. Public key cryptography is used for security together with a distributed secure ledger. Each coin is associated with its current owner's public key. When bitcoins are sent by an owner, a transaction is created, attaching the new owner's public key to the sent coins. The transaction is signed with the previous owner's (the sender's) private key. When this transaction is broadcast to the bitcoin network,

the new owner of these coins is publicized. The signature on the message verifies that the message is authentic. The complete history of transactions is kept by everyone, so anyone can verify current ownership of coins. The approach works by having a public ledger in the form of a blockchain replicated and viewable by all. Each block contains a timestamp and a link to a previous blockchain. Every ten minutes new transactions have to be secured as a block and added to the public blockchain. They are then considered cleared. Peers called data miners compete to create a message hash of the new transaction block such that it cannot subsequently be altered. SHA256 is used as the underlying cryptographic hash function. To make the problem harder there are constraints on the form of the hash code. Thus the problem becomes finding a suitable key that will generate a compliant hash code. The data miner who completes first is rewarded with bitcoins. A majority of miners have to agree that the hash is correct before it is accepted. Once accepted, the new block is added to the chain and cannot ever be altered. This stops fraudulent activity. The approach is considered very secure. However there have been breaches [74]. Ethereum [75], a platform for smart contracts, is taking a similar approach and the traditional banking sector is now interested in the technology [76, 77]. An issue however is that the blockchain as implemented with Bitcoin is based on anonymity of users. This would not be acceptable for the traditional banking sector. Therefore a modified version of the approach where the identities of users are knowable would be necessary. There have been questions about scalability too [78, 79].

4.5 Enterprise security modelling and security as a service

Given the wide range of attacks and the various mechanisms available to counteract them, we see how important it is for enterprises to devote attention to their security profile. An organizational security model which maps business processes, application systems, systems software, servers, and network topology against possible attacks and their defenses provides a good foundation for security management. This is particularly pertinent now that enterprises are moving their infrastructure to the cloud which increases, while at the same time obscuring, the network complexity. Establishing the correct security services involves detailed analysis of need, and sound knowledge of all relevant system components and processes. Making these entities explicit creates a better overall understanding.

Aulkemeier et al. [80] have produced a service-oriented e-commerce reference architecture based on the three layers of technology, application and business. Relevant system components are specified at each level. Their architecture does not contain a security model but it is well placed to form the basis on which a security model could be built. Luhach, Dwivedi and Jha [81] proposed a logical security framework for the small- and medium-sized e-commerce systems. The proposed logical security framework is based on a service-oriented architecture model of e-commerce transactions. The framework includes authentication certificates, code filters, web services SOAP access, HTTPS, IDS, IPS, access control rules, database protection and encryption as well as having business data on a separate server to the e-commerce site. The use of a service-oriented and architecture-centric approach for security engineering can lead to the development of more secure service-oriented applications. The approach develops clearer understanding and exploits security solution reuse where applicable. Dikanski and Abeck [82] developed a service-oriented security architecture view model, with a security engineering view for development artifacts, a security service view for security services, and a security integration view for the integration and centralization of an organization's security infrastructure.

From viewpoint of service engineering, the composition of services into applications in the Internet of Services (IoS) raises further questions on security and trust. Can discovered services be trusted and are they secure? Security preservation within a composition of services is important. Dwivedi and Rath [83] considered six security patterns, Identification and Access Management (IAM), Check Point, Data Confidentiality, Policy, Proxy-Based Firewall, and Secure Service Proxy and proposed to incorporate security features in a service-oriented architecture with the help of software security patterns. This scheme

is described by developing an architectural model integrated with security goals and security patterns. The structural and behavioral aspects of web services composition incorporated with security features were presented using a Unified Modeling Language class diagram and sequence diagram respectively. Formal validation technologies can have a decisive impact for the trust and security of services composition. Armando et al. [84] developed a validation platform which is an integrated toolset for the formal specification and automated validation of trust and security of service-oriented architectures. The goal was to ensure global security of dynamically composed services and their integration into complex architectures by developing an integrated platform of automated reasoning techniques and tools.

The development of architectural models for enterprise security, particularly those based on service-oriented architecture, increases understanding and can yield a solid framework to support future requirements such as handling increasing numbers of attacks, knowledge transfer, technology upgrade, system migration or moves to outsourcing. .

Analysing security requirements systematically leads to the prospect of adopting Security as a Service (SECaaS) [85, 86]. SECaaS is a business model in which a large service provider integrates their security services into a corporate infrastructure thereby providing security as a service for the corporation on the basis that this is a more cost-effective solution. In this scenario, security is provided as a cloud service. Typical security service provision include authentication, anti-virus, anti-malware/spyware, intrusion detection, and security event management. In 2011 the Cloud Security Alliance [87] identified the following areas as feasible SECaaS offerings: identity and access management; data loss prevention; web security; email security; security assessments; intrusion management; security information and event management; encryption; business continuity and disaster recovery; and network security.

The cloud SECaaS market is growing rapidly [88]. Advantages of outsourcing security to the cloud include cost, consistency, uniformity, more reliable virus definition updates, greater security expertise and fewer security administrative tasks. An issue is that each security request would require an exchange with the security provider exposing the request to a possible network attack but secure communication should mitigate this. Furthermore with current trends such as mobile and location independent working the on-premises in-house maintenance of uniform security becomes very difficult. SECaaS may offer an attractive means to manage enterprise security. Additionally cloud services can be developed to share information about attacks and defenses and well as to provide extra resource to fighting attacks when needed (see Section 4.2).

4.6 User education and engagement

The role of training and education in the fight against security breaches has long been recognized. In 2003, The National Institute of Standards and Technology (NIST) proposed a learning continuum model for information security, starting from awareness, through training to education [89]. Their model focused on enhancing security knowledge for end-users. As cyberattacks increase, the role of education and training is becoming increasingly important. The British Retail Consortium [90] produces guidance for retailers on how to protect their online systems. Some non-profit organizations such as the Anti-Phishing Work Group (APWG) and the US Computer Emergency Readiness Team (US-CERT) offer educational interventions to enhance public understanding of the threats posed by attackers and how to protect systems from attacks. Significant efforts have made to provide user education to enable public understanding of security. Such efforts must be sustained.

Previous research has shown that well designed end-user security education can be effective in mitigating against IT infrastructure issues [91, 92, 93]. This could be in the form of web-based training materials, contextual training, and embedded training to enhance users' ability to avoid attacks. It is argued by Kirlappos and Sasse [94] that the aim of security education should be on the drivers of end-user behavior

rather than on warning users of dangers. This means that a well-designed security education should develop threat perception so that users become genuinely aware of the danger. Amankwa, Loock, and Kritzinger [95] discussed the development of end-user education, training and awareness programmes by categorizing known models for enhancing security education, training and awareness based on the stakeholder domains, which included end-users, institutions, and industry. They acknowledged the fact that approaches for enhancing end-users' security knowledge exist but that there has been insufficient research on models for enhancing security knowledge of end-users based on need.

Aware that attacks cannot be prevented by technology alone, researchers have devoted attention to the development of innovative educational media based on the principle that user engagement and education provide a powerful means of preventing electronic attacks, both at the employee and customer levels [96, 97]. Arachchilage, Tahrini and Love [98] investigated how one can develop a mobile game that, through increasing motivation, enhances users' avoidance behavior in order to protect themselves against phishing attacks. The study was based on the notion that computer games offer a natural learning environment which motivates the user to continue whilst also providing education to users. The results from their study showed a significant improvement of participants' phishing avoidance behavior and suggested that participants' threat perception, safeguard effectiveness, self-efficacy, perceived severity and perceived susceptibility positively impact threat avoidance behavior, whereas safeguard cost had a negative impact on it.

It is important that employees and users are educated, encouraging them to be vigilant at all times. They should be taught what qualifies as sensitive data and how to identify threats and avoid them. Acceptable use and security policies must be promoted and enforced at organizational level. It is also crucial that end-users understand their role and responsibilities in maintaining the organization's compliance with relevant regulations operating in its domain. In short, educating the work force is critical and is a key requirement of information security standards such as ISO27001. There are a number of ways that security awareness training can be delivered to end-users. The most popular tends to be the e-learning variety, where online courses covering the essentials of security awareness are mandated for all employees. In this way users are taught they are potential targets and they learn how to look out for social engineering and phishing, increase password security, handle sensitive data, as well as about any specific compliance-driven requirements.

5. Conclusion

This paper has provided a review of current threats and solutions facing e-business and in particular e-commerce. Phishing remains a dominant attack and in particular spear fishing where individual employees or organizations are targeted. It is extremely important that employees and organizations are trained in how to recognize and counter such attacks. User engagement and education is therefore a vital component of the e-business security defense response. Increased collaboration and sharing of attack information is also important. Cloud computing can offer a useful means of facilitating this. Scalable use of resources to counter DDoS attacks offers a useful direction of travel, together with the development of machine learning algorithms for better and quicker recognition of new attacks and anomalies in usage patterns.

References

[1] Anti-Phishing Working Group. Phishing activity trends report. 4th Quarter 2016. [Online available at: http://docs.apwg.org/reports/apwg_trends_report_q4_2016.pdf accessed 13-03-2017].

[2] Symantec. 2016 Internet Threat Report. 2016. [Online available at: https://www.symantec.com/security-center/threat-report accessed 13-03-17].

[3] Anti-Phishing Working Group. Phishing Activity Trends Report. 2nd Quarter 2014. [Online available at: http://docs.apwg.org/reports/apwg_trends_report_q2_2014.pdf accessed 26-02-2016].

[4] Moghimi M, Varjani AY. New rule-based phishing detection method. Expert systems with applications. 2016 Jul 1;53:231-42.
[5] Li L, Berki E, Helenius M, Ovaska S. Towards a contingency approach with whitelist-and blacklist-based anti-phishing applications: what do usability tests indicate? Behaviour & Information Technology. 2014 Nov 2;33(11):1136-47.
[6] Gupta S, Singhal A, Kapoor A. A literature survey on social engineering attacks: Phishing attack. In: Computing, Communication and Automation (ICCCA), 2016 International Conference on. 2016 Apr 29 (pp. 537-540). IEEE.
[7] Udo GJ. Privacy and security concerns as major barriers for e-commerce: a survey study. Information Management & Computer Security. 2001 Oct 1;9(4):165-74.
[8] Hartono E, Holsapple CW, Kim KY, Na KS, Simpson JT. Measuring perceived security in B2C electronic commerce website usage: A respecification and validation. Decision Support Systems. 2014 Jun 30;62:11-21.
[9] Jotwani V, Dutta A. An analysis of E-Commerce security threats and its related effective measures. International Journal. 2016 Jun;4(6).
[10] Ficco M, Rak M. Intrusion tolerance of stealth DoS attacks to web services. In: IFIP International Information Security Conference 2012 Jun 4 (pp. 579-584). Springer, Berlin, Heidelberg.
[11] Kapoor A, Mathur R. Predicting the future of stealth attacks. In Virus Bulletin Conference 2011 Oct (pp. 1-9).
[12] Kalutarage HK, Shaikh SA, Wickramasinghe IP, Zhou Q, James AE. Detecting stealthy attacks: Efficient monitoring of suspicious activities on computer networks. Computers & Electrical Engineering. 2015 Oct 31;47:327-344.
[13] Kiountouzis E. Approaches to the security of information systems. Information Systems Security, New Technologies Publications, Athens, Greece. 2004.
[14] Bonneau J, Herley C, Van Oorschot PC, Stajano F. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In: Security and Privacy (SP), 2012 IEEE Symposium on. 2012 May 20 (pp. 553-567). IEEE.
[15] Darwish A, El-Gendy MM, Hassanien AE. A new hybrid cryptosystem for Internet of Things applications. In: Multimedia Forensics and Security 2017 (pp. 365-380). Springer International Publishing.
[16] Anwar S, Zain JM, Zolkipli MF, Inayat Z, Jabir AN, Odili JB. Response option for attacks detected by intrusion detection system. In: Software Engineering and Computer Systems (ICSECS), 2015 4th International Conference on. 2015 Aug 19 (pp. 195-200). IEEE.
[17] Dworkin MJ. SHA-3 standard: Permutation-based hash and extendable-output functions. Federal Inf. Process. Stds. (NIST FIPS)-202. 2015 Aug 4.
[18] Adams C, Farrell S, Kause T, Mononen T. Internet X. 509 public key infrastructure certificate management protocol (CMP). 2005.
[19] Jain AK, Ross AA, Nandakumar K. Introduction. In: Introduction to Biometrics. 2011 (pp. 1-49). Springer US.
[20] Duarte T, Pimentão JP, Sousa P, Onofre S. Biometric access control systems: A review on technologies to improve their efficiency. In: Power Electronics and Motion Control Conference (PEMC), 2016 IEEE International. 2016 Sep 25 (pp. 795-800). IEEE.
[21] Sabharwal M. The Assessment of Concerns, Opinions and perceptions of bank customers to find the significant metrics for deployment of biometrics in e-banking. Assessment. 2016 Apr;140(5).
[22] Carpenter D, McLeod A, Hicks C, Maasberg M. Privacy and biometrics: An empirical examination of employee concerns. Information Systems Frontiers. 2016:1-20.

[23] Li QY, Zhang L. The public security and personal privacy survey: Biometric technology in Hong Kong. IEEE Security & Privacy. 2016 Jul;14(4):12-21.
[24] National Population Commission, Nigeria. Nigeria Over 167 million population: Implication and Challenges. 2016. [Online available at: http://www.population.gov.ng/index.php/84-news/latest/106-nigeria-over-167-million-population-implications-and-challenges accessed 07/26/2016].
[25] Biometric Update. Nigeria. 2017. [Online available at: http://www.biometricupdate.com/tag/nigeria accessed 08/08/2017].
[26] James A, Shehu Y. Security and Integrity of Fingerprint Templates. Project. Researchgate. 2017. [Online available at: https://www.researchgate.net/project/Security-and-Integrity-of-Fingerprint-Templates accessed 08/08/2017].
[27] Le C, Jain R. A survey of biometrics security systems. EEUU. Washington University in St. Louis. 2009.
[28] Jain AK, Hong L, Pankanti S, Bolle R. An identity-authentication system using fingerprints. Proceedings of the IEEE. 1997 Sep;85(9):1365-88.
[29] Savvides M, Kumar BV, Khosla PK. Cancelable biometric filters for face recognition. In: Pattern Recognition, 2004. ICPR 2004. Proceedings of the 17th International Conference on 2004 Aug 23 (Vol. 3, pp. 922-925). IEEE.
[30] Mathivanan B, Palanisamy V, Selvarajan S. Multi dimensional hand geometry based biometric verification and recognition system. Int J Emerg Technol Adv Eng. 2012;2(7):348-54.
[31] Daugman J. How iris recognition works. IEEE Transactions on circuits and systems for video technology. 2004 Jan;14(1):21-30.
[32] Dere SN, Gurjar AA, Sipna CO. Human identification using palm-vein images: A new trend in biometrics. International Journal of Engineering Science. 2016 Mar;2298.
[33] Jain AK, Ross A, Prabhakar S. An introduction to biometric recognition. IEEE Transactions on circuits and systems for video technology. 2004 Jan;14(1):4-20.
[34] Mazaira-Fernandez LM, Álvarez-Marquina A, Gómez-Vilda P. Improving speaker recognition by biometric voice deconstruction. Frontiers in bioengineering and biotechnology. 2015;3
[35] Monaco J. Robust keystroke biometric anomaly detection. U.S. Army Research Laboratory Aberdeen Proving Ground, MD 21005, USA. 2016. [Online available at: https://arxiv.org/abs/1606.09075 accessed 08/08/2017].
[36] Parkhi OM, Vedaldi A, Zisserman A. Deep face recognition. In:BMVC 2015 Sep (Vol. 1, No. 3, p. 6).
[37] Simonyan K, Vedaldi A, Zisserman A. Learning local feature descriptors using convex optimisation. IEEE Transactions on Pattern Analysis and Machine Intelligence. 2014 Aug;36(8):1573-85.
[38] Parkhi OM, Simonyan K, Vedaldi A, Zisserman A. A compact and discriminative face track descriptor. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition 2014 (pp. 1693-1700).
[39] Taigman Y, Yang M, Ranzato MA, Wolf L. Deepface: Closing the gap to human-level performance in face verification. In: Proceedings of the IEEE conference on computer vision and pattern recognition. 2014. (pp. 1701-1708).
[40] Taigman Y, Yang M, Ranzato MA, Wolf L. Web-scale training for face identification. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition 2015 (pp. 2746-2754).
[41] Schroff F, Kalenichenko D, Philbin J. Facenet: A unified embedding for face recognition and clustering. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition 2015 (pp. 815-823).

[42] Sun Y, Liang D, Wang X, Tang X. Deepid3: Face recognition with very deep neural networks. arXiv preprint arXiv:1502.00873. 2015 Feb 3.
[43] Flores M, Torres G, Garcia G, Licona M. Fingerprint verification methods using Delaunay triangulations. Int. Arab J. Inf. Technol.. 2017 May 1;14(3):346-54.
[44] Yang W, Hu J, Wang S. A Delaunay triangle-based fuzzy extractor for fingerprint authentication. In: Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on. 2012 Jun 25 (pp. 66-70). IEEE.
[45] Ross A, Jain A, Reisman J. A hybrid fingerprint matcher. Pattern Recognition. 2003 Jul 31;36(7):1661-73.
[46] Deng H, Huo Q. Minutiae matching based fingerprint verification using delaunay triangulation and aligned-edge-guided triangle matching. In: Audio-and Video-Based Biometric Person Authentication 2005 (pp. 357-372). Springer Berlin/Heidelberg.
[47] Silva AG, Barbosa IA, Nascimento MV, Rego TG, Batista LV. Analysis of the Performance Improvement Obtained by a Genetic Algorithm-based Approach on a Hand Geometry Dataset. In: Proceedings of the International Conference on Artificial Intelligence (ICAI) 2015 Jan 1 (pp. 125-130).
[48] Park G, Kim S. Hand biometric recognition based on fused hand geometry and vascular patterns. Sensors. 2013 Feb 28;13(3):2895-910.
[49] Daugman J. Evolving Methods in Iris Recognition and Implications from 200 Billion Iris Comparisons. Presentation. The First International Conference on Biometrics: Theory, Applications and Systems (BTAS 07). 2017. [Online available at: http://www.cse.nd.edu/BTAS_07/John_Daugman_BTAS.pdf accessed 08-08-2017].
[50] Daugman JG. High confidence visual recognition of persons by a test of statistical independence. IEEE transactions on pattern analysis and machine intelligence. 1993 Nov;15(11):1148-61.
[51] Roy K, Bhattacharya P, Suen CY. Iris recognition using shape-guided approach and game theory. Pattern Analysis and Applications. 2011 Nov 1;14(4):329-48.
[52] Bouraoui I, Chitroub S, Bouridane A. Does independent component analysis perform well for iris recognition? Intelligent Data Analysis. 2012 Jan 1;16(3):409-26.
[53] Tsai CC, Lin HY, Taur J, Tao CW. Iris recognition using possibilistic fuzzy matching on local features. IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics). 2012 Feb;42(1):150-62.
[54] Chen Y, Liu Y, Zhu X, He F, Wang H, Deng N. Efficient iris recognition based on optimal subfeature selection and weighted subregion fusion. The Scientific World Journal. 2014;2014.
[55] Zhang D, Guo Z, Lu G, Zhang L, Liu Y, Zuo W. Online joint palmprint and palmvein verification. Expert Systems with Applications. 2011 Mar 31;38(3):2621-31.
[56] Lee JC. A novel biometric system based on palm vein image. Pattern Recognition Letters. 2012 Sep 1;33(12):1520-8.
[57] Sun J, Abdulla W. Palm vein recognition using curvelet transform. In: Proceedings of the 27th Conference on Image and Vision Computing New Zealand 2012 Nov 26 (pp. 435-439). ACM.
[58] Al-Juboori AM, Bu W, Wu X, Zhao Q. Palm vein verification using Gabor filter. International Journal of Computer science issues. 2013 Jan;10(1):678-84.
[59] Al-Juboori AM, Bu W, Wu X, Zhao Q. Palm vein verification using multiple features and locality preserving projections. The Scientific World Journal. 2014 Feb 17;2014.
[60] Mehrotra H, Vatsa M, Singh R, Majhi B. Does iris change over time?. PloS one. 2013 Nov 7;8(11):e78333.
[61] James A, Obande G, Bentahar K, Development-of-a-secure-BioPKI-using-Palm-Vein-Technology. Project. Researchgate. 2017. [Online available at:

https://www.researchgate.net/project/Development-of-a-secure-BioPKI-using-Palm-Vein-Technology accessed 09-08-2017].
[62] Vasiliadis G, Polychronakis M, Ioannidis S. MIDeA: a multi-parallel intrusion detection architecture. In: Proceedings of the 18th ACM conference on Computer and communications security 2011 Oct 17 (pp. 297-308). ACM.
[63] Jiang H, Zhang G, Xie G, Salamatian K, Mathy L. Scalable high-performance parallel design for network intrusion detection systems on many-core processors. In: Proceedings of the ninth ACM/IEEE symposium on Architectures for networking and communications systems. 2013 Oct 21 (pp. 137-146). IEEE Press.
[64] Jamshed MA, Lee J, Moon S, Yun I, Kim D, Lee S, Yi Y, Park K. Kargus: a highly-scalable software-based intrusion detection system. In: Proceedings of the 2012 ACM conference on Computer and communications security 2012 Oct 16 (pp. 317-328). ACM.
[65] Bul'ajoul W, James A, Pannu M. Improving network intrusion detection system performance through quality of service configuration and parallel technology. Journal of Computer and System Sciences. 2015 Sep 30;81(6):981-99.
[66] Bul'ajoul W, James A, Shaikh S, Pannu M. Using CISCO network components to improve NIDPS performance. Third International Conference on Computer Science & Engineering. Computer Science & Information Technology (CS & IT) 2017:6(10):137-157. 201 . [Online available at: http://airccj.org/CSCP/vol6/csit65712.pdf accessed 08-08-2017].
[67] Buczak AL, Guven E. A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials. 2016 Jan 1;18(2):1153-76.
[68] Tran TP, Nguyen TT, Tsai P, Kong X. BSPNN: boosted subspace probabilistic neural network for email security. Artificial Intelligence Review. 2011 Apr 1;35(4):369-82.
[69] Feng W, Zhang Q, Hu G, Huang JX. Mining network data for intrusion detection through combining SVMs with ant colony networks. Future Generation Computer Systems. 2014 Jul 31;37:127-40.
[70] Kalutarage HK, Shaikh SA, Zhou Q, James AE. Sensing for suspicion at scale: A Bayesian approach for cyber conflict attribution and reasoning. In: Cyber conflict (CYCON), 2012 4th international conference on 2012 Jun 5 (pp. 1-19). IEEE.
[71] Pilkington M. Blockchain Technology: Principles and Applications. In: Olleros FX and Zhegu, M, editors. Research Handbook on Digital Transformations. Edward Elgar, 2016. [Online available at: https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2662660 accessed 08-08-2017].
[72] Lansiti M, Lakhani KR. The truth about blockchain. Harvard Business Review. 2017 Jan 1;95(1):119-27.
[73] Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. 2008. [Online available at: https://bitcoin.org/bitcoin.pdf accessed 08-08-2017].
[74] Morabito V. The security of blockchain systems. In: Business Innovation Through Blockchain 2017 (pp. 61-78). Springer International Publishing.
[75] Wood G. Ethereum: A secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper. 2014 Apr;151.
[76] Financial Times. Blockchain can create financial sector jobs as well as kill them. 2016. [Online available at: https://www.ft.com/content/3a9ef8d8-33d5-11e6-bda0-04585c31b153 [accessed 08-08-2017].
[77] PwC . Blockchain technology: Is the banking sector ready for FinTech? 2016. [Online available at: http://pwc.blogs.com/fintech/2016/11/blockchain-technology-is-the-banking-sector-ready-for-fintech.html accessed 13-03-2017].

[78] Croman K, Decker C, Eyal I, Gencer AE, Juels A, Kosba A, Miller A, Saxena P, Shi E, Sirer EG, Song D. On scaling decentralized blockchains. In: International Conference on Financial Cryptography and Data Security 2016 Feb 26 (pp. 106-125). Springer Berlin Heidelberg.
[79] Vukolić M. The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In: International Workshop on Open Problems in Network Security 2015 Oct 29 (pp. 112-125). Springer, Cham.
[80] Aulkemeier F, Schramm M, Iacob ME, Van Hillegersberg J. A service-oriented e-commerce reference architecture. Journal of theoretical and applied electronic commerce research. 2016 Jan;11(1):26-45.
[81] Luhach AK, Dwivedi SK, Jha CK. Implementing the logical security framework for E-commerce based on service-oriented architecture. In: Proceedings of International Conference on ICT for Sustainable Development 2016 (pp. 1-13). Springer Singapore.
[82] Dikanski A, Abeck S. A view-based approach for service-oriented security architecture specification. In: The Sixth International Conference on Internet and Web Applications and Services, St. Maarten, The Netherland Antilles 2011 Mar.
[83] Dwivedi AK, Rath SK. Incorporating security features in service-oriented architecture using security patterns. ACM SIGSOFT Software Engineering Notes. 2015 Feb 6;40(1):1-6.
[84] Armando A, Arsac W, Avanesov T, Barletta M, Calvi A, Cappai A, Carbone R, Chevalier Y, Compagna L, Cuéllar J, Erzse G. The AVANTSSAR platform for the automated validation of trust and security of service-oriented architectures. Tools and Algorithms for the Construction and Analysis of Systems. 2012:267-82.
[85] Sharma DH, Dhote CA, Potey MM. Security-as-a-Service from Clouds: A comprehensive Analysis. International Journal of Computer Applications. 2013 Jan 1;67(3).
[86] Furfaro A, Garro A, Tundis A. Towards security as a service (secaas): On the modeling of security services for cloud computing. In: Security Technology (ICCST), 2014 International Carnahan Conference on 2014 Oct 13 (pp. 1-6). IEEE.
[87] Cloud Security Alliance. Security guidance for critical areas of focus in cloud computing v3. 0. Cloud Security Alliance. 2011:15.
[88] Cloud Pro. The rise of cloud-based security is an indication of how trustworthy cloud computing has now become. 2014. [Online available at: http://www.cloudpro.co.uk/cloud-essentials/cloud-security/3671/security-as-a-service-really-has-become-a-no-brainer accessed 12-03-17].
[89] Wilson M, Hash J. Building an information technology security awareness and training program. NIST Special publication. 2003 Oct;800(50):1-39.
[90] British Retail Consortium. Cyber Security Toolkit: A Guide for Retailers. 2017. [Online available at: http://brc.org.uk/media/120731/brc-cyber-security-toolkit_final.pdf accessed 14-03-2017].
[91] Jafari S. Enhancing security culture through user-engagement: An organisational perspective. International Journal of ICT Research in Africa and the Middle East (IJICTRAME). 2017 Jan 1;6(1):31-39.
[92] Kennedy SE, Kennedy SE. The pathway to security–mitigating user negligence. Information & Computer Security. 2016 Jul 11;24(3):255-64.
[93] Le Compte A, Elizondo D, Watson T. A renewed approach to serious games for cyber security. In Cyber conflict: Architectures in cyberspace (CyCon), 7th international conference on 2015 May 26 (pp. 203-216). IEEE.
[94] Kirlappos I, Sasse MA. Security education against phishing: A modest proposal for a major rethink. IEEE Security & Privacy. 2012 Mar;10(2):24-32.
[95] Amankwa E, Loock M, Kritzinger E. A conceptual analysis of information security education, information security training and information security awareness definitions. In Internet Technology

and Secured Transactions (ICITST), 2014 9th International Conference for 2014 Dec 8 (pp. 248-252). IEEE.
[96] Arachchilage NA, Love S, Beznosov K. Phishing threat avoidance behaviour: An empirical investigation. Computers in Human Behavior. 2016 Jul 31;60:185-97.
[97] Sanchez F, Duan Z. A sender-centric approach to detecting phishing emails. In Cyber Security (CyberSecurity), 2012 International Conference on 2012 Dec 14 (pp. 32-39). IEEE.
[98] Arachchilage NA, Tarhini A, Love S. Designing a mobile game to thwarts malicious IT threats: A phishing threat avoidance perspective. arXiv preprint arXiv:1511.07093. 2015 Nov 23.