ISSN 2278-3091
Volume 9, No.1, January – February 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse33912020.pdf
https://doi.org/10.30534/ijatcse/2020/33912020

Cyber Attacks and Impacts: A Case Study in Saudi Arabia

Reem K. Alqurashi, Mohammed A. AlZain, Ben Soh*, Mehedi Masud, Jehad Al-Amri
College of Computers and Information Technology, Taif University, Saudi Arabia
*La Trobe University, Bundoora 3086, Australia.

ABSTRACT

With the development of technology, modern computer-assisted and Internet crimes have been increasing all this while, and there is a need to further investigate the current status of cybercrime and computer forensics in the region. Saudi Arabia is one of the fastest growing countries in the Middle East in terms of communications technologies such as the Internet and mobile phones. In this paper we explore cybercrime challenges in the Middle East using Saudi Arabia as a case study. In particular, we examine the impact of the use of Internet and cybercrime on adolescents in Saudi Arabia.

Keywords: crime, computer, Saudi Arabia, Forensics Technology, interne, future, teenager

1. INDTRODUCTION

With the development of technology, modern computer-assisted and Internet crimes have been increasing all this while. Cybercrime internationally affects the IT environment to a large extent, be it management, companies, banks or individuals[6] [9] [7]. The rapid expansion of the order of techniques has been observed. Information sharing[11] [10] is a major distortion feature of misappropriation of information on the Internet.

The remainder of this paper is organized as follows. Section II discusses the background of computer crimes. Section III lists some types of computer crimes, while Section IV explains the forensic technology on the computer. In the V section we discuss the challenges of cybercrime in the Middle East. In the section VI speaks History of Internet use in Saudi Arabia. In Section VII we explain computer crimes in Saudi Arabia and in Section VIII some cases of attacks in Saudi Arabia and Section IX about cyber criminals in Saudi Arabia and in Section X we explain anti-crime law in Saudi Arabia In section XI we discuss the use of adolescents for the Internet. In the XII section speaks of Islamic criminal law and also in section XIII speaks that Sharia attends cybercrime and in section XIV talk about the future of cybercrime.

2. BACKGROUND: WHAT IS CYBERCRIME?

The term computer crime to refers to criminal activities involving illegal uses of computers. The definition by Eoghan Casey [26] is used in this paper.

Relationships such as "cybercrime," "computer crime," and "network crime" have no unanimously acknowledged definitions. Part of the misunderstanding arising from their use originates from the circumstance that criminals now use computers in the progression of committing almost any crime. Although there is no decided meaning of a computer crime, the denotation of the tenure has developed more detailed over time. A computer crime mentions principally to a wide set of crimes defined in certain laws. These crimes comprise shoplifting of computer amenities; unsanctioned access to protected computers; software piracy and modification or stealing of warehoused information automatically; computer-assisted coercion; and obtaining unauthorized access to records[3] [4] [31] [5] [29]. Circulation in pilfered passwords and broadcast of viruses or destructive instructions also constitute a cybercrime. One of the foremost complications in a computer crime is that when the computer or network is not directly implicated in a crime but digital indication associated to the crime [14] .

However, the roles played by a computer in a cybercrime can be categorized in one of three ways: as a tool, as a storage device, or as a victim [13].

2.1 Computer as a Tool

The computer can be used as a tool to obligate movement crimes. This group embraces those crimes that criminals have conventionally dedicated in the physical world but this is now fashionable with snowballing occurrence on the Internet, such as online mart deception, and pornography circulation. Criminals also use the Internet to encourage an extensive assortment of traditional crime environments that are not available in the “real world”, such as email and chat meetings. Since criminals may use computer networks to carry out traditional crimes in new conducts, steps must be taken to assess prevailing criminal rules to guarantee that what is forbidden in the physical world is correspondingly proscribed in the computer-generated world.

2.2 Computer as a Storage Device

Criminals, such as industries, managements and persons, take benefit of the aptitude of computers to stockpile great quantities of information[8] [12]. Criminals stockpile information when obligating an extensive variability of outdated crimes, and the electronic information develops clues applicable to the internal working of the crime. The use of computers and hardware stowage commonly does not necessitate the construction of new functional regulations, but the need for electronic indication may necessitate a modifications to current commandments overriding law implementation access to such indication [13].

2.3 Computer as a Victim

The computer can also be the board of criminal movement. Frequently described as "network crime," this movement comprises bouts on the security, integrity, or availability of computer systems. Criminals transmit out these occurrences to: (1) acquire information warehoused on the victim's computer without authorization, (2) remove or adapt data or restrict data access with the convenience of a computer or the information it comprises. Criminal activities encompassed in this grouping of computer as a victim are unauthorized access to a computer[29], the announcement of viruses and other malevolent code, distortion of websites, and renunciation of service attacks that cause inconvenience and/or damages to computer systems or data [13].

3. TYPES OF COMPUTER CRIMES

3.1 Spam

E-mail messages are an essential contribution. Often, hacking, design attacks, and malicious attacks on e-mail services are attempted to defraud. Attackers use emails that may have original content with phishing URLs to steal useful data. This kind of email is just spam [28].

3.2 Worms

Computer worms are constructed to broadcast without warning or user interaction, producing an upsurge in traffic service requests that will ultimately lead to cyber-attack. Attacker uses a malevolent worm as a primary tool to target software susceptibilities [25].

3.3 Sniffer

Packet sniffing is the restriction of packets that pass through the network in which they are installed. Sniffer Pack is a tool that monitors all network data, which is easy to use.

Packet sniffers are mostly used by network administrators to help them troubleshoot network problems.

Sniffers are of two types: active and passive. The passive sniffers only collect data and are impossible to detect. Passive sniffers are useful for network management in areas such as telecommunications, radar systems, medical equipment, etc.

Active sniffers operate on other systems through different technologies. For example, a malicious packet can be sent from a compromised host to a legitimate host [18].

3.4 Phishing

Phishing is an activity of endeavoring to obtain data for example usernames, PINs, and credit card particulars (and occasionally, money) by camouflaging as a dependable object in an electronic announcement. Phishing through e-mail deception or immediate messaging guides victims to access a counterfeit website whose appearance and impression are practically indistinguishable to the authentic one [17].

3.5 Denial of service attack

A network grounded renunciation of amenity attack for IP (Internet Protocol) constructed networks. It is prevalently called SYN submerging. It the whole thing by an attacker distribution many TCP (Transmission Control Protocol) joining requirements with tricked foundation discourses to a victim's machine. Each demand reasons the beleaguered host to instantiate data constructions out of an incomplete puddle of possessions. Once the board congregation's resources are bushed, no more received TCP influences can be recognized [30].

3.6 Virus Dissemination

A computer virus is a sequencer that container 'infect' other genuine agendas by adjusting them to comprise a conceivably 'evolved' reproduction of himself. Viruses can banquet themselves, deprived of the information or authorization of the workers, to hypothetically The Internet stretches viruses a predominantly well-organized new pathway for comprehensive contamination. The following figure show relatives and environments of viruses [17].

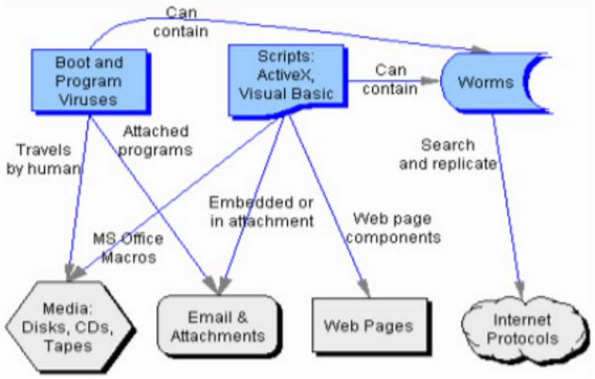

Figure 1 : Viruses – Families and Habitats [17].

3.7 Cyber Stalking

Cyber stalking is fundamentally by means of the Internet to frequently pursue alternative individual. This exasperation could be voluptuous in landscape, or it could have supplementary enthusiasms counting annoyance. Individuals dispensation a lot of info around themselves online. Such info can permission one defenseless to cyber pestering, a period that fundamentally mentions to by means of the Internet to stem (to illegitimately shadow and wristwatch somebody) [20].

3.8 Password Attacks

The goal of a password attack is to also deduction a password or become it finished trust dodges, which are recognized as social engineering. And password attacks consume humble adventures. Most password attacks are envisioned for contravention. However, admission container likewise principal to stealing and destruction. The outbreak must be cautiously deliberate and implemented. A password attack container continuously be confidential as a prearranged category of mistreatment, and the universal physiognomies accompanying with this organization smear. Assumed the dependence on social engineering, which is operating persons in instruction to two-time them from penetrating information such as passwords, the greatest credible method to attack is concluded individual communication. Social engineering category of password attacks contributes to up to 90 % of all such attacks. The individual who is prospective to obligate a password attack is the individual situated neighboring the residence where the attack instigated, as an interior foundation or user [33].

4. COMPUTER FORENSICS TECHNOLOGY

With the speedy expansion of network technology, people's existence has transformed melodramatically. The beginning of the Internet does not deliver coziness. It also delivers a new criminal frequency that fluctuates from the outmoded frequency. In bright of the new network crime, computer forensics technology ascends at the ancient instant. Computer forensics is also called a criminological network study. The indication of the network crime it delivers is documented by commandment and can be secondhand as an operative and dependable basis of sentence. The main attitude in computer forensics [32] is to use the appropriate network information investigation technology to magistrate the motivation of the crime and to accumulate the network crime data of the suspicious specifically, which is engaged as the indication of authorized experimental [27] .

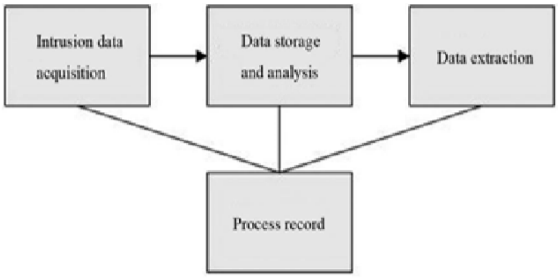

Figure 2:Technical process of computer forensics [27].

As shown in Figure 2, the process of computer forensics technology is divided into three phases [21]. First, information for an interruption is developed. Then the composed information is conserved and investigated. Finally, the evidence and information obtained from the investigation are recorded immediately as a statement. In the three progressions of indication assortment, based on the continuousness attitude of effective indication, it is compulsory to greatest the three progressions [27].

Network interruption information, network interruption is typically an occurrence on a server with a huge quantity of compost information, and the authentic determination of the process is concealed in it for an incursion determination. The communal network occurrence manner is a flood occurrence that is merely uneven and difficult to preserve. The communal flood occurrence methods are User Datagram Protocol (UDP) flood attack, Transmission Control Protocol (TCP) flood attack and Internet Control Messages Protocol (ICMP) flood attack [27] .

The overhead flood occurrences are all DDoS flood occurrences, which flood the server with a huge quantity of compost information, instigating the server to run out of capitals and go downhearted. The difference amongst the three DDoS flooding occurrences declared overhead dishonesties in the different message information used for the occurrence. UDP message mostly occurrences target IP address. TCP mostly uses the TCP protocol to overhang a service. Information for demanding confirmation is uninterruptedly sent to devour server resource. And admittance to other users is blocked. ICMP is a traffic occurrence that devours resources by sending more than 65,535 bytes of information to the server[27].

In order to see the effectiveness of computer forensics, the subsequent three philosophies should be adhered to [19]:

1) The crime scene is cordoned to guarantee the indication (evidence) is not contaminated.;

2) The assortment of indication network truthfulness and continuousness necessity be certain. The final indication succumbed will be the same as the final indication examined.

3) In the complete progression of suggestion assortment, there requirement be a third party to administer so to safeguard the independence of indication [27].

5. CYBERCRIME CHALLENGES IN THE MIDDLE EAST

Progressive communications technologies exposed the entrance to the development of humankind and crime. But lawmaking and congresspersons are continuously leisurewear than the expansion of ICTs, send off our district susceptible to all categories of cyberattacks and will brand it problematic to implement cybercrime laws. Current proceedings demonstrate in the province from Stuxnet to Saudi Aramco's attack that we are nowadays fragment of comprehensive microelectronic skirmishes. [16] .

5.1 Responsibility

In the Middle East, there is an enormous quandary when it comes to cyberspace commandments. When considering cybercrime lawmaking enforceable in the region, there is no management subdivision accountable for conscripting commerce with Internet regulations. Many interventions by the administration may be complicated in Internet-related rules and regulations, such as e-signature, e-commerce, domain name registering, copyright and intellectual property, cybercrime, cyber espionage, and cyber terrorism. The engrossment of more than one management subdivision such as the Department of Business, the Department of Transportation and Info Knowledge, the Department of Internal and Important Bank, the Department of Righteousness, and even the Astuteness and Resistance Departments can be non-existent or in an experimental stage. The problematic confronted by any of the overhead establishments is to prerogative responsibility for such commandments and this will be a challenge. For the Middle East managements when conscripting cybercrime commandment. It is significant to create an enthusiastic management subdivision to arrangement with Internet commandments. [15] [16] .

5.2 Organizational Structure

One of the main challenges in the district is intersection, specifically in production with cybercrime subjects. Cybercrime necessitates a momentous development of administrative constructions to be in residence comprised of strong relationships of orientation. It will be problematic to comportment compound researches that necessitate the backing of changed permissible and methodological professionals. In the Middle East there are correspondingly struggles and nonexistence of association among many performers to confrontation cybercrime. Commandment implementation interventions are principally unassisted in contending cybercrime. Collaboration among dissimilar performers in cybercrime lawmaking must be lectured in command to progress the administrative construction to struggle cybercrime [16].

5.3 Technical Capabilities

There is a large predicament when it originates to administrative procedures for cybercrime researches. There is correspondingly a badly-behaved in preserving the truthfulness of digital indication throughout an examination since it is continuously imperative in a criminal circumstance, but the countryside of the suggestion in cybercrime brands this commission more problematic. Police brigadiers can effortlessly extinguish digital suggestion in cybercrime cases by means of constant procedures of uneasiness and imprisonment. Commandment management brigadier's expression a foremost challenge beforehand attractive respondents, who will requirement to divulge where and who the criminal is. Because cybercrime is a transcontinental crime, the probabilities of pursuing miserable respondents can be very problematic if not incredible. Shots to improved pathway distinctiveness online pose thoughtful complications for concealment supporters and central to partisan responses that are standard in the Middle East. I comprehend that it will be a large challenge for commandment administration officials since they may contemplate campaigners to be cyber criminals when commentary cybercrime. I recommend declaring your administrative technique in any online commandment particularly when commerce with digital suggestion. Commandment administration must be accomplished in the modern performances for considering cybercrime [16] **.**

5.4 Education

One of the furthermost significant fundamentals in contesting cybercrime is education and consciousness. Inappropriately, around is no operative approach or proposal to advance volume construction and safekeeping education in the area. There are insufficient concrete operations in Qatar, UAE, Oman and Saudi Arabia in the area of cybercrime education. Cybercrime lawmaking is not the individual resolution to competition cybercrime. It is fragment of superior cyber security approach which also necessitates better-quality instruction and consciousness movements. Administrations must progress their volume construction and education of their workforce and inhabitants to better confrontation cybercrime[16] .

5.5 Legislative Capabilities

Legislation is fragment of the approach to contest cybercrime and not the complete explanation. The badly-behaved is that when representative's arrangement with cybercrime belongings, they will attempt to smear commonplace jurisdictional procedures that may embrace municipal, criminal, and monitoring commandment. It capacity labor in an insufficient belonging but it will not labor in entirely belongings of cybercrime, specifically crimes constructed on the Internet. Electronic lawmaking or connected commandments are feeble or absentminded in the region. Smooth contemporary cybercrime commandments cannot be painstaking complete and dependable to transaction with cybercrime, expressly at the phase of examination, which is one of the furthermost multifaceted stepladders. The following MENA countries in the region have cybercrime laws or a system to deal with cybercrime starting from the year indicated [15]:

UAE: Federal Law No.2 of 2006
Saudi Arabia: Cybercrime System (2007)
Jordan: Cybercrime temporary law (2010)
Syria: Cybercrime and Communication on the Internet (2012)
Oman: Cybercrime Law (2011)

It is better for managements to learn from the Assembly of Europe and attempt to sanction the Assembly of Europe's Cybercrime Agreement. They organize not requirement to copy and paste, first they requirement to comprehend and then smear the measures and drawn from the blow convention microelectronic commandments that encounter their necessities and in agreement with the Universal Declaration of Humanoid Privileges[16].

6. CASE STUDY: INTERNET USE AND CYBERSECURITY IN SAUDI ARABIA

The Internet has a justly young history in 1997 in Saudi Arabia when Internet service became accessible to countries in Saudi Arabia. It's an old-fashioned of possession? Conferring to an twelve-monthly report organized by the Communications and Information Technology Commission (CITC) in Saudi Arabia in 2016, there was a noteworthy increase in Internet admittance in the country from 47% to 74.9% from 2011 to the end of 2016 respectively [34] [1].

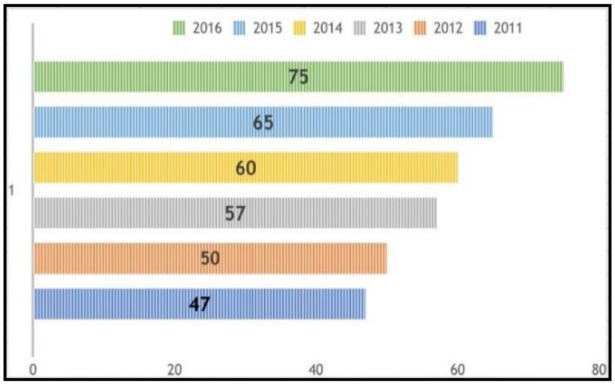

Figure 3: The increasing use of the internet in Saudi Arabia.

The country's populace is projected at 3 million, and the projected number of internet users predictable at 24 million people, demonstrations that at least 75% of the total populace has internet admittance. The CITC report of 2016 also designates that due to the development of the use of internet podiums and submissions such as social media and internet-based games, the request for broadband and internet services has intensely increased [34] [1].

Internet and ICT use in the country is accompanying to services and is anticipated to intensification even more than we have seen in current years. As such, information security will become an indispensable requirement for 75% of the total populace of Saudi Arabia who frequently admittance the Internet. Saudi Arabia's digital transformation blueprint lists information security and cybersecurity as some mechanisms that will be an integral fragment of the expansion of the use of Internet-based services in the country. The approach comes at a time when Saudi Arabia is seeing an increasing number of establishments, which seek answers to information security execution [1].

This, in calculation to the snowballing volume for intercontinental internet connectivity, generates a noteworthy question that is transported about by

the stable intensification in the mandate for internet use within KSA [1].

Since the commencement of 2005, the Internet service in Saudi kingdom saying the principal and most important process of rearrangement where the Convention of Preachers Steadfastness issued rule number 229 on 28/09/2004 in order to re-organize the internet provision in SA. Which led to the spreading of tasks to numerous appropriate organizations to advance service and promotion their effectiveness (Warf and Vincent, 2007).

Complete, internet service is provided by [2] :

1. Infrastructures and Information Technology Department is accountable for all the superintendent and supervisory roles concerning the internet services.
2. Data Service Providers (DSP's), including Saudi Telecom Company are accountable for the operative characteristics of the network package filter (filtering).
3. King Abdul-Aziz City for Science and Technology (KACST) has continuous delivery of the link service to the internet for theoretical and research purposes and is responsible for management interventions if needed,
4. Service breadwinners to the internet: Deliver the connection to the Internet for administration subdivisions, establishments, establishments, and persons. (King Abdul-Aziz city for Science and Technology, 2014) [2].

6.1 Computer crimes in Saudi Arabia

Information technology in the Arab world has been a great impact in the last century, with 15.8 million internet users in Saudi Arabia at the end of 2012. Field surveys in Saudi Arabia carries out by the Communications and Information Technology Commission estimated more than one user per mobile broadband subscription. Demand for Internet services is expected to increase by more than SAR 2.6 billion in 2012, approximately SAR 3.6 billion in 2012. They experienced financial losses in Saudi Arabia in 2012 and suffered financial losses of $195 (approximately SAR 730). It is rated on 40% of the study in Saudi Arabia. That's their computer [17]. Almost all Middle Eastern countries have electronic laws. It requires an appropriate law to deal with cybercrime that complies with Islamic law, commensurate with the large number of Muslims in the Arab world. In general, computer crimes started from piracy programs.

Government transactions in Saudi Arabia involve almost all computers, whether in circulation regulator, communications, power, fitness info system or passport. Any compromise on the security of the management system can do great damage. Cybercrime is fragment of or complicated in "conventional crimes" such as medication transferring, individuals running and money cleaning. What threatens young Saudis is that they are genuinely complicated in such crimes, but also commonly do not vacillate to use the Internet to obligate dissimilar kinds of crimes, from replication information to promoting drugs and pornography [23].

6.2 Cases of cyber-attacks in Saudi Arabia

Three examples of recent cyber-attacks in Saudi Arabia are given below:

1- State oil company Aramco came under cyberattack. More than 30,000 computers in Saudi oil company Aramco was hit by a virus in August 2012 and resulted in the demolition of

information and drives to computers. The attack was meant to stop oil production (World Exchange Report, 2013).
2- King Saud University (KSU) has been hacked by some unidentified hacker. It is a community university in Riyadh.
3- The government administration in Saudi Arabia was hacked by a succession of heavy cyber-attacks, which temporarily disrupted the government operations until attacks were stopped (Al-Arabiya, 2013) [17] .

6.3 Cyber laws of Saudi Arabia

Paper about Saudi Arabia Cyber commandment conditions mentioned that any individual who is complicated in Construction, groundwork, communication, or storing of substantial encroaching on community instruction, spiritual standards, community moralities, and confidentiality, concluded the data network or computers will be question to incarceration for a historical not elsewhere five years and a well not beyond three million riyals or also [22] .

6.4 The Anti -Crime Act in Saudi Arabia

Lawmaking is the backbone of each civilization. Laws, accompanied by ethical conscience, can lead to a less non-violent world. It is a safe way to produce a civilization and make a country an appropriate place to live and connect with others. Therefore, it is very important that we have laws on cybercrime that represents a problem and a threat to social life because laws could act as a preventive measure to committing these cybercrimes. And there is a singular circumstance in terms of authorizations approved in the Koran and Sunnah in Saudi Arabia. The Koran and Sunnah did not mention laws and penalties imposed in computer crimes, but the Koran and Sunnah mentioned general penalties such as shoplifting, manslaughter, disloyalty and other penalties, so the anti-crime law exists but does not mention cybercrimes. The resulting damage regulates the level of each crime.
Aimed at sample (stealing of bank accounts and stealing of private photos or videos from the computer) decrease underneath a low stealing but there are dissimilar properties for each, so there must be different consequences for each. In most countries in the region, children must be at least 18 years old to be deemed an adult, while in Saudi Arabia the 15-member Shura Council proposes that children be less than 15 years old. Internet services in Saudi Arabia also run websites that spread pornography and tarnish Islamic values (www.internet.gov.sa)
The crime of cyber terrorism falls under the influence of corruption[23] .

6.5 Internet Uses by Saudi Teenagers

Some research into teenagers use of the Internet has focused principally on its impression on character construction. However, detailed research has absorbed on the role of fathers in manipulating their teenagers' use of the Internet. For this determination, Use of the Internet and the transitional role-played by maternities in the process. It principally relies on nonfiction on maternal inspirations on teenagers' use of the Internet. Some literature scrutinizes the encouragement of parentages on children's use of the Internet in Saudi Arabia. Overview of teenagers' use of the Internet, the belongings on teenagers' socialization and maternal inspirations on teenagers' use of the Internet [2] .

6.5.1 Progenies and internet usage

In a report of the European Union Children's Online Survey, it is recommended that 60% of children between the ages of 9 and 16 use the Internet daily, while 30% use the Internet at least weekly. However, the Internet has become a prevalent cybernetic location and location
for many happenings. Zotova and Zinchenko (2014), the Internet will become an encouragement in management the relationship between people in society. Internet access does not occur among the populace. Help us create new lines of announcement, but it is a social impression. You can connect with children, youth, learning and network. Will have possessions on their social, psychological and physical health. Until you use the Internet, you can be an operative elector in distribution ideas, as well as permitting students to physique specific communities. It is likely to build or accompaniment social capital and develop the aptitude of young people to cope with threats or jeopardies. It is whispered to be a risk to children. High digital capability leads to a digital culture This cultural experience must be in need of ethical performance and safety standards
For example, you might be exposed to fighting between nudity, disagreeable language and criminal ideas.

6.5.2 Consequences of Internet Use for Children

The nonfiction says that there are many compensations to using the Internet by children. However, the probable negative impressions of the Internet on children make it compulsory to guarantee that children are well endangered from these effects. Reasonable Internet use. Bleakly et al. (2016) reported that intellectual communication methods have been used by many investigators to investigate the harmful or challenging Internet use of people. The challenging use of the Internet is accompanying with negative relational and psychosocial outcomes (Caplan and High, 2011 in Mleakly et al., 2016). In children and young people, challenging Internet use is accompanying with increased rates of consideration deficit hyperactivity complaint (Yoo et al., 2004), sleep sicknesses, afternoon overindulging (Choi et al., 2009) and poor academic presentation (Jacobsen and Forste, 2011). The negative impression of problematic use of the Internet on children and young people makes the need to mediate the use of the Internet for risky children. The use of the Internet not only unfavorably affects children's personal lives, but also in most cases these negative effects can be protracted to comprise general connection and interactions with other people. Through social networking, young people create new associations and reinforce existing ones [2] .

6.6 Islamic Criminal Code

Muslim ministers belittle nonspiritual permissible systems that are functional in numerous Muslim republics, for example in Jordan, they have not fashioned an another standpoint but unclear and universal philosophies. Dissimilar categories of crimes, counting cybercrime, remained disregarded. This, of progression, creates a possible danger to cyberspace, since the islamic law (Shariah's) attitude of criminalization conditions. It is mentioned in quran 'And nor will we punishing pending we had directed them an Apostle' (Qur'an 17:15). It is unspoken that the crimes and chastisements must not be functional retroactively. If no rejoinder in Shariah, then cyber criminals and Muslim hackers who dedicated cybercrime can seepage persuasion [24] .

6.7 Shariah prohibits Cyber crime

Shariah does not clearly proscribe any sympathetic of cybercrime, then it prepares cover universal instructions of criminalization. Rendering to the fundamentalists, the additional foundation of Shariah regulation, (the Prophet Tradition) delivers important provision for the criminalization of cybercrime. Researchers have mentioned a number of Hadiths, aimed at sample, the Prophet said 'No damage will be perpetrated [on anyone] nor communal [in contradiction of anyone]' to criminalise developing crimes. The Hadith delivers a permissible foundation for criminalizing cybercrime [24].

7. THE FUTURE OF CYBERCRIME

Cybercrime has an unpredictable future judging from the trends where the culprits always end up a step ahead of the authorities. Cyber criminals always come up with a new way of committing the crimes. Authorities have to increase the skill levels if they hope to catch up with cybercrime offenders. Cyber criminals seem always to find a new way of defrauding people.

Growth of cybercrimes shows that there is a high chance that it would continue growing. Currently, traditional laws and technical protection are no longer enough against computer crimes.

8. CONCLUSION

With the development of technology, modern computer-assisted and Internet crimes have been increasing all this while, and there is a need to further investigate the current status of cybercrime and computer forensics in the Middle East, particularly Saudi Arabia. In this paper we explored cybercrime challenges in Saudi Arabia. In particular, we examine the impact of the use of Internet and cybercrime on adolescents in Saudi Arabia.

REFERENCES

[1] H. Agil, COPYRIGHT AND INTERNET LAWS IN SAUDI ARABIA" THE NEED OF IMPROVEMENT.

[2] A. Almogbel, Parental Influences on the Internet Use by Children in Saudi Arabia, (2019).

[3] M. A. AlZain, Data security, data management and performance evaluation in a multi-cloud computing model, (2014).

[4] M. A. AlZain, A. S. Li, B. Soh and M. Masud, Byzantine Fault-Tolerant Architecture in Cloud Data Management, International Journal of Knowledge Society Research (IJKSR), 7 (2016), pp. 86-98. https://doi.org/10.4018/IJKSR.2016070106

[5] M. A. AlZain, A. S. Li, B. Soh and M. Masud, Managing Multi-Cloud Data Dependability Faults, Knowledge-Intensive Economies and Opportunities for Social, Organizational, and Technological Growth, IGI Global, 2019, pp. 207-221.

[6] M. A. Alzain and E. Pardede, Using multi shares for ensuring privacy in database-as-a-service, 2011 44th Hawaii International Conference on System Sciences, IEEE, 2011, pp. 1-9. https://doi.org/10.1109/HICSS.2011.478

[7] M. A. AlZain, E. Pardede, B. Soh and J. A. Thom, Cloud computing security: from single to multi-clouds, 2012 45th Hawaii International Conference on System Sciences, IEEE, 2012, pp. 5490-5499.

[8] M. A. AlZain, B. Soh and E. Pardede, A byzantine fault tolerance model for a multi-cloud computing, 2013 IEEE 16Th International Conference On Computational Science And Engineering, IEEE, 2013, pp. 130-137.

[9] M. A. AlZain, B. Soh and E. Pardede, Mcdb: using multi-clouds to ensure security in cloud computing, 2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing, IEEE, 2011, pp. 784-791. https://doi.org/10.1109/DASC.2011.133

[10] M. A. AlZain, B. Soh and E. Pardede, A new approach using redundancy technique to improve security in cloud computing, Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), IEEE, 2012, pp. 230-235.

[11] M. A. AlZain, B. Soh and E. Pardede, A new model to ensure security in cloud computing services, Journal of Service Science Research, 4 (2012), pp. 49-70.

[12] M. A. AlZain, B. Soh and E. Pardede, A survey on data security issues in cloud computing: From single to multi-clouds, Journal of Software, 8 (2013), pp. 1068-1078. https://doi.org/10.4304/jsw.8.5.1068-1078

[13] I. Carr, Computer crime, Routledge, 2017.

[14] E. Casey, Digital evidence and computer crime: Forensic science, computers, and the internet, Academic press, 2011.

[15] M. N. El Guindy and F. Hegazy, Cybercrime Legislation in The Middle East, 2014.

[16] M. Elguindy, Cybercrime Challenges in Middle East, 2012.

[17] B. M. E. Elnaim, Cyber crime in Kingdom of Saudi Arabia: The threat today and the expected future, Information and Knowledge Management, 2013, pp. 14-19.

[18] C. Gandhi, G. Suri, R. P. Golyan, P. Saxena and B. K. Saxena, Packet sniffer–a comparative study, International Journal of Computer Networks and Communications Security, 2 (2014), pp. 179-187.

[19] D. Gugelmann, F. Gasser, B. Ager and V. Lenders, Hviz: HTTP (S) traffic aggregation and visualization for network forensics, Digital Investigation, 12 (2015), pp. S1-S11.
https://doi.org/10.1016/j.diin.2015.01.005

[20] A. B. Hassan, F. D. Lass and J. Makinde, Cybercrime in Nigeria: causes, effects and the way out, ARPN Journal of Science and Technology, 2 (2012), pp. 626-631.

[21] F. Karpisek, I. Baggili and F. Breitinger, WhatsApp network forensics: Decrypting and understanding the WhatsApp call signaling messages, Digital Investigation, 15 (2015), pp. 110-118.

[22] N. K. Khan, Cyber laws encompassing the Security of E-Quran in Saudi Arabia.

[23] N. K. Khan, Taxonomy of Cyber Crimes and Legislation in Saudi Arabia, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 1 (2012), pp. 207.

[24] A. Maghaireh, Shariah Law and cyber-sectarian conflict: how can Islamic Criminal Law respond to cyber crime?, (2009).

[25] B. K. Mishra and A. Prajapati, Cyber Warfare: Worms' Transmission Model, International Journal of Advanced Science and Technology, 63 (2014), pp. 83-94.
https://doi.org/10.14257/ijast.2014.63.08

[26] R. Moore, Cybercrime: Investigating high-technology computer crime, Routledge, 2014.

[27] Y. Qi, Computer Real-Time Location Forensics Method for Network Intrusion Crimes, IJ Network Security, 21 (2019), pp. 530-535.

[28] S. B. Rathod and T. M. Pattewar, Content based spam detection in email using Bayesian classifier, 2015 International Conference on Communications and Signal Processing (ICCSP), IEEE, 2015, pp. 1257-1261.

[29] H. Samra, A. Li, B. Soh and M. Al Zain, Utilisation of hospital information systems for medical research in Saudi Arabia: A mixed-method exploration of the views of healthcare and IT professionals involved in hospital database management systems, Health Information Management Journal (2019), pp. 1833358319847120.
https://doi.org/10.1177/1833358319847120

[30] C. L. Schuba, I. V. Krsul, M. G. Kuhn, E. H. Spafford, A. Sundaram and D. Zamboni, Analysis of a denial of service attack on TCP, Proceedings. 1997 IEEE Symposium on Security and Privacy (Cat. No. 97CB36097), IEEE, 1997, pp. 208-223.

[31] G. K. Sodhi, G. S. Gaba, L. Kansal, E. Babulak, M. AlZain, S. K. Arora and M. Masud, Preserving Authenticity and Integrity of Distributed Networks through Novel Message Authentication Code, Indonesian Journal of Electrical Engineering and Computer Science, 12 (2018), pp. 1297-1304.
https://doi.org/10.11591/ijeecs.v12.i3.pp1297-1304

[32] M. Vallentin, V. Paxson and R. Sommer, {VAST}: A Unified Platform for Interactive Network Forensics, 13th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 16), 2016, pp. 345-362.

[33] O. Wori, Computer crimes: factors of cybercriminal activities, International Journal of Advanced Computer Science and Information Technology, 3 (2014), pp. 51-67.

[34] E. I. M. Zayid and N. A. A. Farah, A study on cybercrime awareness test in Saudi Arabia-Alnamas region, 2017 2nd International Conference on Anti-Cyber Crimes (ICACC), IEEE, 2017, pp. 199-202.
https://doi.org/10.1109/Anti-Cybercrime.2017.7905290