# A Review of New Trends in Cyber Attacks:A Zoom into Distributed Database Systems

**Conference Paper** · January 2018

CITATIONS
11

READS
1,247

**2 authors**, including:

Attlee M. Gamundani
Namibia University of Science and Technology
**58** PUBLICATIONS **216** CITATIONS

SEE PROFILE

IST-Africa 2018 Conference Proceedings
Paul Cunningham and Miriam Cunningham (Eds)
IIMC International Information Management Corporation, 2018
ISBN: 978-1-905824-59-5

# A Review of New Trends in Cyber Attacks: A Zoom into Distributed Database Systems

Attlee M. GAMUNDANI, Lucas M. NEKARE
*Namibia University of Science and Technology, 13 Storch Street, Windhoek, 9000, Namibia*
*Email: agamundani@nust.na, mbambolucas4@gmail.com*

**Abstract:** The recent mushrooming of new terminology for cyber-attacks signals latest trends that attackers are capitalizing on. The impact of such attacks has left many of the affected victims grounded or literally financially handicapped. As many of the security professionals are always on their toes trying to keep pace with the bad guys, it seems it is always an infinite war. Indeed there is a call for more vigilance when it comes to cyber security. It is against this background that this paper is formulated with a focus on distributed database systems. An analysis on the new trends in cyber-attacks on distributed database systems were done with a focus on identifying new trends and their effects. A desktop approach on expert reports, articles and books was employed to populate this review paper. New trends in cyber-attacks are differentiated from predecessor cyber-attack trends by looking at corresponding features that an attack possesses and the vulnerabilities being explored by attackers using new trends. An impact analysis of the new trends in cyber attacks is also presented in summary against the CIA security triad. A key business value of this research is it's relevant input data towards design of security solutions for distributed database systems and many related disciplines that directly and indirectly depend on distributed system designs.

**Keywords:** Attack, Cyber, Database, Distributed, and Trends.

## 1. Introduction

The emergency of new cyber attacks left many security professionals with more questions than answers. The main challenge identified by this research was the absence of state of the art review of the new trends in cyber attacks across many industries. The focus on distributed database systems was on the basis of their wide target by attackers as they house valuable data for many large organisations that became victim to recent cyber attacks worldwide.

New trends in cyber-attacks have been witnessed lately, which were compromising different application platforms including but not limited to Distributed Database Systems (DDS). Cyber-attacks have been exiting for many years since the internet was born [1]. Recent cyber-attacks have added new features that make them more unique from the previous cyber-attacks, hence the new trends. What makes the trends new in the recent cyber attacks are the salient features being used to exploit possible vulnerabilities.

### *1.1 – Distributed Database Systems (DDS)*

Distributed Database Systems can be classified based on the architecture, application, and hierarchy. DDS architecture can be peer to peer or client-server[2]. DDS can refer to a computer system that interconnect a number of databases that are located physically across various locations to make the distribution transparent to users [3]. By virtue of this distribution, the impact of cyber attacks can be distributed as well hence technically demanding. The Distributed Database Management System (DBMS) is the software that

 

manages DDS [4], once attacked it will render the whole DDS grounded as it becomes the single point of failure.

As discussed by [5], vulnerabilities that exists in distributed database systems and how to eliminate them, requires more than just abstract threat models which capture neither realistic databases nor realistic attack scenarios, hence the need for more practical solutions.

In a study based on distributed database security strategy by [6]–[8] indicates how to ensure security on distributed database management systems in an open network environment. Security strategies and implementation of security policy by [9], clearly shows that security in databases is quite a wide domain that demands a holistic approach. Considering the new trends in cyber security, these noble suggestions have not been effective either.

### *1.2 – An overview of Cyber Attacks*

A cyber-attack is an attempt by hackers to disrupt, damage, destroy or malfunction a computer system or network or interrupt the flow of computer data [10]. This is also supported by [11] as an attack performed from one computer against another computer system or a website. Some of the obvious examples of cyber-attacks on DDS are:- Distribution Denial of Services (DDoS), SQL injections (SQL databases). In addition to DDoS there are three type of DDoS attacks that have been discovered in 2015[12], namely; MS-SQL, BitTorrent and Port mapper. Hackers need to build a list of devices' IP addresses that are accessible freely online by everyone. Hackers obtain these IP addresses by spoofing them. Infected devices will be directed via command. The hackers send a query to the devices then redirect the large responses to a target device [13].

An attacker can use unauthorized access to gain access to database systems and alter, publish, destroy or sell private information[14],[15]. Private information can be a victim's financial details, health information, personal details (names, address, date of birth, etc.) and private life information[16]. Most of cyber-attacks on distributed database systems compromises business clients' information[17](financial information or personal information).

In the work of [18], a description of cyber-attacks is given three dimensions which could be classified as: - (1) unofficial access or unauthorized access; (2) data corruption, alteration or destroyer (3) user system fake messages. What will be lacking in these classifications will be the ability to identify the new trends in cyber-attacks; an analysis of how the new trends occur and compromises DDS as well as measuring the impact of each attack.

### *1.3 – Why new trends in cyber attacks?*

Distributed database systems are vulnerable to new trends in cyber-attacks. New trends in cyber-attacks are being formed based on the new discovered zero-day vulnerabilities in distribution database systems. According to [19], modern cyber-attacks are often conducted across multiple vectors and stages. Advanced new trends in cyber-attacks are designed to evade and escape traditional network security[19]. Analysing these new trends in cyber attacks on DDS will help understand how attackers are implementing the new trends; it will help to identify the vulnerabilities explored by these trends, hence make the work of security professionals well informed.

## 2. Objectives

The main key objectives that guided this research work are outlined below:

1. Identify new trends in cyber-attacks targeting and compromising distributed database systems.
2. Assess the features of the new trends in cyber-attacks.

3. Evaluate the impacts caused by the new trends in cyber attacks on distributed database systems.

## 3. Methodology

A qualitative research approach was employed through desktop research. As guided by [20] on qualitative research, reviewing of books, articles and studies from experts in the field of computer security based on their recent findings mostly work published in 2017 was the primary strategy for the research. The state of the art work was reviewed based on the year of publication (2017 up to date) and the other search parameters employed were based on the domain (distributed database systems & cyber attacks).

Collected information was analysed to identify new features that point towards the new trends in cyber-attacks hence drawing a line between previous known trends that might have been solved before. From the reviewed articles we can conclude that we had a fair representation on the trends as we didn't limit our search to scholarly articles but also considered technical reports for technology magazines online, which are faster in disseminating information as and when it is available.

Impacts caused by the new trends in cyber-attacks were analysed based on the CIA triad. CIA triad consists of Confidentiality, Integrity and Availability. All security measures are designed to protect CIA triad of the information in the system as highly supported by [21]–[25].

## 4. Cyber Attacks in Distributed Database Systems

### *4.1 – New Penetration attacks*

This attack was performed by identifying a vulnerability on the Equifax's website that allowed them to obtain a file from the website then used it to gain access to the database. The attackers managed to gain privileges to siphon millions of sensitive data from the company's database [26]. The breach at Equifax was scaled 10 on the scale of 1 to 10 if we apply the framework by [27], which entails that, the breach had a high impact on the database system.

### *4.2 – NotPetya*

According to [28], "A global cyber-attack spread across the world, hitting computer systems everywhere from the UK and Russia to America and Ukraine." The ransom ware infected more computer systems in Britain, Russia and Dutch firms [28]. The ransom ware was known as NotPetya. NotPetya obtained its name because it was not a variant of Petya according to [29].

### *4.3 – Petya*

Petya was a ransom ware that started spreading on June 27, 2017 and infected many organizations in more countries worldwide. Petya was the first ransom ware before NotPetya, this ransom ware had similar features but just slightly different from NotPetya. Petya was designed based on WannaCry ransom ware [30]. They all explore the same vulnerabilities with slight differences[31], [32]. Figure 1, gives a summary of the top 20 affected countries based on the number of firms affected [33].

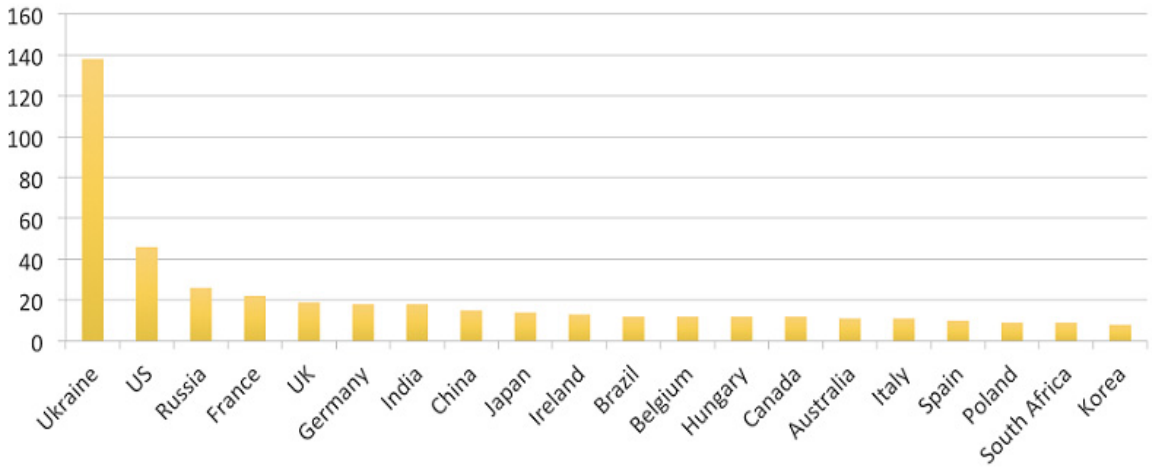


*Figure 1. Top 20 affected countries based on the number of firms affected[33].*

*4.4 – Toxic Trojan*

A Trojan that was distinguished as a Firefox extension. The Trojan used the Firefox extension to communicate the URL path for the C&C server to its malware minions [34]. The Firefox extension masks the malware as a security feature. The comments that are used to communicate with the control servers include hash tags. Moreover, [34], highlighted that backdoor Trojan used comments on the "Baby one more time" singer's post to find the control server that sends and receives data from infected computers. The malware extension has been distributed using a compromised Swiss security website. Lastly this extension enabled the *Turla* gang to read directory content, download and upload files from and to the C&C server and execute files on the infected system [34].

*4.5 – Phishing Whaling*

Whaling is a phishing technique that was used to target high profile business managers, executives and even celebrities [35], [36]. According to [37], "it is different from ordinary phishing in that with whaling, the email or webpages serving the scam take on a more official or serious looking." Normal phishing techniques use social media sites to get the credential details of the victim. Whaling attack can also be considered as Spear phishing, because the attackers target a specific person or company.

*4.6 – DDos Black Nurse*

Black Nurse was a new DoS that could take down servers and firewalls using a single computer [38]. Security researchers [39]–[42], may be quoted to relate towards the evident features of Black Nurse as one that allows a hacker to spend less effort to launch large-scale attacks. Servers and Firewalls can be taken down offline with less effort and one laptop. It overloads firewalls and shut them down with low-volume ICMP (Internet Control Message Protocol) base attack. Black Nurse overload the central processors and render them useless with ICMP error message to servers and firewalls [38].

*4.7 – Mongo DB ransom*

According to [43], Mongo DB database systems were attacked by a ransom ware named Mongo DB ransom. More than 27 000 database systems were attacked in few hours, which doubled by the end of the day. Hackers run the ransom to gain access to the database so that they can copy and delete data. The Mongo DB ransom exploits bad configurations and unpatched database systems[43]–[45]. The attacker required administrators to pay certain amount of money in order to get their data back. The hacker required 0.2 bit coin (US$ 184)[43].

*4.8 – Trojan Virus*

Trojan viruses install themselves in a computer and give administrator access to the creator of the Trojan[46]–[49]. The latest Trojan was modified with the new abilities to propagate themselves to other computers in the network. Hackers used these Trojans to create zombies to perform a DDoS sometimes. Trojan virus can be used to compromise distributed database systems[50] in a number of ways.

*4.9 – Machine Language Enabled*

Machine language is used to link up different tools together that can be used when conducting a cyber-attack[51]. Tools are linked in such a way that one-tool collects information then feed it to other tools. The other tools will analyse the information then process the output and pass it to another tool or use information to attack a system. For instance, if one tool finds a user password, it passes the password to another tool to conduct the attack on a specific system. The other tool will also try to find other systems that use the same password[51]. Furthermore, Machine language allows hackers to program set of tools that can communicate and act like human beings[52]. These toolsets can conduct a research about the system on their own and perform appropriate attacks. Toolset can conduct phishing techniques against a company or individual. These toolsets are designed with the abilities to evade detection and block methods in use[51].

*4.10 Man-in-the Middle attack*

In September 07, 2017 AXA insurance company portal was breached and about 5400 customers' personal data were compromised [53]. The breach compromised customers' email addresses, mobile numbers and date of birth. The data were compromised when users attempted to log in their portals. The portal uses one-time passwords (OTPs)[53]. As a result, the hacker managed to intercept the information. One of the contributing factors to the breach was the website which was not secured until after the breach[53]. This attack was classified as man in the middle because the hacker obtained the requests and responds from the website to get the details. A new trend here is that, the hacker did not have to be in the same network (Wi-Fi) with the victim to intercept the data as before, only needed to be in the flow of traffic between a client and the server to intercept the information. A hacker need to intercept a public key and can transpose his own credentials [54].

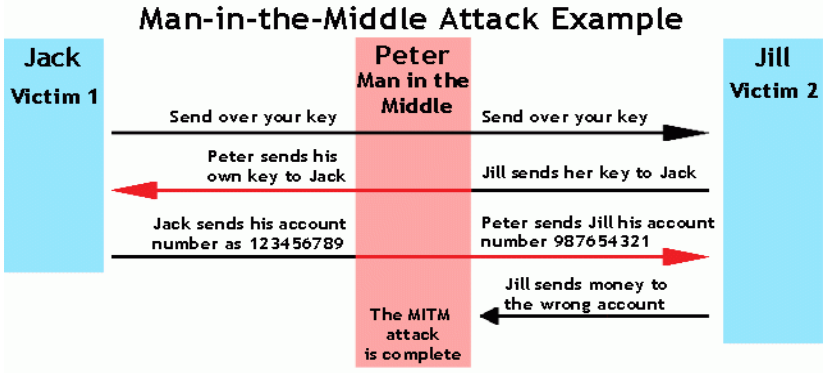


*Figure 3. Man in the middle[54].*

*4.11 Credential Theft*

Nearly 29 million users registered with Latin American social network accounts were compromised. According to [55], the website had posted a notification that says "We suffered an external attack that compromised the security of our databases and the code of Taringa!" Passwords were hashed with "weak MD5" algorithm [55]. MD5 hashing algorithm is considered as an out-dated algorithm [56],[57]. In few days nearly 27 million hashed passwords were cracked. Apart from the mentioned data no other data have been

compromised[58]. The social media then notified its users to change their passwords as soon as possible.

## 5. Findings and Analysis

Table 1 highlights some of the noticeable new trends on the attacks identified in section 4 as compared to their previous attack features if any.

*Table 1: A highlight of new trends in cyber attacks as compared to the previous attack features*

| Cyber-attack | New Trends in Cyber-attacks | Previous attack features |
|---|---|---|
| Penetration | Use vulnerabilities existing in third parties' software. Obtaining valuable files from the system. | Use SQL injections and Trojans. |
| Ransom ware (Petya, NotPetya and WannaCry) | Ability to replicate worldwide. Ability to scramble system files. Fast replication and affect computer in the same network. | Need user interaction to affect the computer or network. Not fast enough to affect computers worldwide. |
| DDoS (Black Nurse) | Only one or two computer to render the whole system down. Can take down servers and firewalls using a single computer | Need to use more than two computers. |
| Phishing (Whaling) | Clone the website login page and create domain name similar to the victim. | Only uses email and text messages or calls. |
| Trojan (Toxic Trojan and Trojan Virus) | Uses browser extension (Firefox). Control servers through social media comments hash tags. Can propagate themselves to other computer in the network | Need users to install it in the computer in order to control the victim computer. Do not have the ability to propagate to other computers themselves |
| Machine Language Enabled | Uses a group of tools to evade detection and to bypass firewall | |
| Mongo DB ransom | Exploits the security vulnerabilities that exist in Mongo DB. | |
| Credential theft | New tools to decrypt hashed passwords. | Need plain text credentials. |

## 6. Summary

An impact review of the identified new trends in cyber attacks are now assessed based on the CIA security triad as summarized in Table 2. The shaded section indicates the impact of the identified attack and their new trends. Some sections may not be shaded for a particular attack, like for instance, credential theft, under availability, it doesn't necessarily imply that such an attack has no effect when it comes to availability but the severity of the attack under that consideration is minimal.

*Table 2: Impact of new trends in cyber attacks*

| Cyber-attack | Confidentiality | Integrity | Availability |
|---|---|---|---|
| Penetration attack | | | |
| Whaling | | | |
| Credential theft | | | |
| NotPetya | | | |
| Petya | | | |
| WannaCry | | | |
| MITM | | | |
| Trojan Virus | | | |
| Machine Language enabled attack | | | |
| Toxic Trojan | | | |

| | | | |
|---|---|---|---|
| Black Nurse | | | |
| Mongo DB ransom | | | |

## 7. Business Benefits

A clear business value from this work in being able to employ the recent data to formulate viable security solutions not only for distributed database systems but also for various distributed system platforms. Most of the identified and summarized cyber attacks and their key trends cut across many disciplines. Clever investments options into the security portfolio for many entities will be enhanced and informed decisions can be made from the findings here presented.

Besides providing state of the art updates on cyber attacks to security professionals, this paper can be used an awareness campaign by organisations towards security of their systems across the organisational units.

## 8. Conclusions

This paper summarizes some of the cyber-attacks that possess new features, which makes them different from previous cyber-attack trends as presented in Table 1. However this cannot be concluded as an exhaustive list but representative enough to draw some key conclusions, on observed trends so far.

Lastly, an impact review of the new attack trends against the CIA security triad were summarized in Table 2, which gives an entry level into the security discussions when considering design of practical solutions for an organisation or individuals. It is the expectation of the authors that this preliminary work towards building literature for new trends in cyber attacks will gain mileage and more interest, as the quest for practical solutions towards cyber welfare is no more a secret across board.

As a recommendation, security professionals and researchers from both the EU and Africa can collaborate on the subject of cyber attacks and create a living lab towards cyber security solution designs and state of the art dissemination of information in a timely manner. This can be an on-going project as cyber attacks are continuously on the increase as new technology trends are also being developed, hence demanding a fresh look into the cyber security horizon.

## References


[1] K. K. R. Choo, "The cyber threat landscape: Challenges and future research directions," *Comput. Secur.*, vol. 30, no. 8, pp. 719–731, 2011.

[2] R. Schollmeier, "A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications," in *Proceedings - 1st International Conference on Peer-to-Peer Computing, P2P 2001*, 2001, pp. 101–102.

[3] L. Frank, "Architecture for integrating heterogeneous distributed databases using supplier integrated e-commerce systems as an example," in *2011 International Conference on Computer and Management, CAMAN 2011*, 2011.

[4] T. Mahmood and U. Afzal, "Security Analytics: Big Data Analytics for Cybersecurity," in *2013 2nd National Conference on Information Assurance (NCIA)*, 2013, pp. 129–134.

[5] P. Grubbs, T. Ristenpart, and V. Shmatikov, "Why Your Encrypted Database Is Not Secure," in *Proceedings of the 16th Workshop on Hot Topics in Operating Systems - HotOS '17*, 2017, pp. 162–168.

[6] Z. S. Zubi, "On distributed database security aspects," *2009 Int. Conf. Multimed. Comput. Syst.*, 2009.

[7] M. T. QUASIM, "Security Issues in Distributed Database System Model," *An Int. J. Adv. Comput. Technol.*, vol. 2, no. Xii, pp. 396–400, 2013.

[8] M. Firdhous, "Implementation of Security in Distributed Systems - A Comparative Study," *Int. J. Comput. Inf. Syst.*, vol. 2, no. 2, p. 6, 2011.

[9] M. C. Murray, "Database Security: What Students Need to Know," *J. Inf. Technol. Educ.*, vol. 9, pp. 61–77, 2010.

[10] H. Lin, "Offensive Cyber Operations and the Use of Force," *J. Natl. Secur. Law Policy*, vol. 4, no. 1, pp. 63–86, 2010.
[11] V. Farhat, B. Mccarthy, and R. Raysman, "Cyber Attacks : Prevention and Proactive Responses," *Practical Law*, pp. 1–12, 2011.
[12] N. Hoque, D. K. Bhattacharyya, and J. K. Kalita, "Botnet in DDoS Attacks: Trends and Challenges," *IEEE Commun. Surv. Tutorials*, vol. 17, no. 4, pp. 2242–2270, 2015.
[13] X. Zhang, A. Tsang, W. T. Yue, and M. Chau, "The classification of hackers by knowledge exchange behaviors," *Inf. Syst. Front.*, vol. 17, no. 6, pp. 1239–1251, 2015.
[14] M. Cremonini and D. Nizovtsev, "Risks and Benefits of Signaling Information System Characteristics to Strategic Attackers," *J. Manag. Inf. Syst.*, vol. 26, no. 3, pp. 241–274, 2009.
[15] R. Popa and C. Redfield, "CryptDB: Processing queries on an encrypted database," *Commun. ...*, vol. 55, no. 9, p. 103, 2012.
[16] J. Lindamood, R. Heatherly, M. Kantarcioglu, and B. Thuraisingham, "Inferring private information using social network data," *Proc. 18th Int. Conf. World wide web WWW 09*, vol. 10, p. 1145, 2009.
[17] B. Zhu, A. Joseph, and S. Sastry, "A taxonomy of cyber attacks on SCADA systems," in *Proceedings - 2011 IEEE International Conferences on Internet of Things and Cyber, Physical and Social Computing, iThings/CPSCom 2011*, 2011, pp. 380–388.
[18] A. Bamrara, "Evaluating database security and cyber attacks: A relational approach," *J. Internet Bank. Commer.*, vol. 20, no. 2, 2015.
[19] X. Chen, M. Scott, and D. Caselden, "New Zero-Day Exploit targeting Internet Explorer Versions 9 through 11 Identified in Targeted Attacks « Threat Research Blog | FireEye Inc," *FireEye Blogs*, 2014. [Online]. Available: https://www.fireeye.com/blog/threat-research/2014/04/new-zero-day-exploit-targeting-internet-explorer-versions-9-through-11-identified-in-targeted-attacks.html.
[20] S. A. McLeod, "Qualitative vs Quantitative Data | Simply Psychology," *Simply Psychology*, 2017. [Online]. Available: https://www.simplypsychology.org/qualitative-quantitative.html.
[21] T. Chia, "Confidentiality, Integrity, Availability: The three components of the CIA Triad," *English*, 2012. [Online]. Available: http://security.blogoverflow.com/2012/08/confidentiality-integrity-availability-the-three-components-of-the-cia-triad/.
[22] C. Perrin, "The CIA Triad," *TechRepublic*, p. 1, 2008.
[23] G. S. Haughn Matthew, "What is confidentiality, integrity, and availability (CIA triad)? - Definition from WhatIs.com," *techtarget.com*, 2014. [Online]. Available: http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA.
[24] Infosec, "CIA Triad," *infosec*, 2017. [Online]. Available: http://resources.infosecinstitute.com/category/certifications-training/cissp/domains/security-and-risk-management/the-security-cia-triad/#gref.
[25] Y. Sattarova Feruza and T. H. Kim, "IT security review: Privacy, protection, access control, assurance and system security," *Int. J. Multimed. Ubiquitous Eng.*, vol. 2, no. 2, pp. 17–32, 2007.
[26] N. Perlroth, "Equifax Says Cyberattack May Have Affected 143 Million Customers - The New York Times," *New York Times*, pp. 7–11, 2017.
[27] A. Litan, "The Five Layers of Fraud Prevention and Using Them to Beat Malware," *Management*. pp. 1–9, 2011.
[28] A. Foster, "Global cyber attack latest: What we know so far as cyber attack spreads | World | News | Express.co.uk," *Express*, 2017. [Online]. Available: https://www.express.co.uk/news/world/821945/global-cyber-attack-latest-news-Ukraine-WPP-Europe-what-we-know-so-far. [Accessed: 20-Jan-2018].
[29] G. Smyth, "Using data virtualisation to detect an insider breach," *Comput. Fraud Secur.*, vol. 2017, no. 8, pp. 5–7, 2017.
[30] C. Graham, "NHS cyber attack: Everything you need to know about 'biggest ransomware' offensive in history," *Telegr.*, no. May, pp. 1–11, 2017.
[31] S. Mohurle and M. Patil, "A brief study of Wannacry Threat : Ransomware Attack 2017," *Int. J. Adv. Res. Comput. Sci.*, vol. 8, no. 5, pp. 2016–2018, 2017.
[32] A. Green, "Ransomware and the GDPR," *Netw. Secur.*, vol. 2017, no. 3, pp. 18–19, 2017.
[33] Symantec Security Response, "What you need to know about the WannaCry Ransomware | Symantec Connect Community," *Symantec Official Blog*, 2017. [Online]. Available: https://www.symantec.com/connect/blogs/what-you-need-know-about-wannacry-ransomware.
[34] Millman Rene, "Russian hackers used Britney Spears' Instagram posts to control malware," *SC Media*, 2017. [Online]. Available: https://www.scmagazineuk.com/russian-hackers-used-britney-spears-instagram-posts-to-control-malware/article/667180/. [Accessed: 20-Jan-2018].
[35] V. R. Hawanna, V. Y. Kulkarni, and R. A. Rane, "A novel algorithm to detect phishing URLs," in *International Conference on Automatic Control and Dynamic Optimization Techniques, ICACDOT 2016*, 2017, pp. 548–552.

[36] S. Gupta, A. Singhal, and A. Kapoor, "A literature survey on social engineering attacks: Phishing attack," in *Proceeding - IEEE International Conference on Computing, Communication and Automation, ICCCA 2016*, 2017, pp. 537–540.
[37] P. Gil, "What Is Whaling and How Does the Internet Attack Work?," *Lifewire*, 2017. [Online]. Available: https://www.lifewire.com/what-is-whaling-2483605. [Accessed: 20-Jan-2018].
[38] Ashok India, "BlackNurse: New DDoS attack launched via a single laptop can bring down firewalls and servers," *International Business Times*, 2016. [Online]. Available: http://www.ibtimes.co.uk/new-ddos-attack-method-called-blacknurse-lets-hackers-take-down-firewalls-servers-single-laptop-1592214. [Accessed: 20-Jan-2018].
[39] Q. Yan, F. R. Yu, Q. Gong, and J. Li, "Software-defined networking (SDN) and distributed denial of service (DDOS) attacks in cloud computing environments: A survey, some research issues, and challenges," *IEEE Communications Surveys and Tutorials*, vol. 18, no. 1. pp. 602–622, 2016.
[40] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDOS) flooding attacks," *IEEE Commun. Surv. Tutorials*, vol. 15, no. 4, pp. 2046–2069, 2013.
[41] A. Saied, R. E. Overill, and T. Radzik, "Detection of known and unknown DDoS attacks using Artificial Neural Networks," *Neurocomputing*, vol. 172, pp. 385–393, 2016.
[42] N. Hoque, H. Kashyap, and D. K. Bhattacharyya, "Real-time DDoS attack detection using FPGA," *Comput. Commun.*, vol. 110, pp. 48–58, 2017.
[43] D. Pauli, "MongoDB ransom attacks soar, body count hits 27,000 in hours • The Register," *The Register*, 2017. [Online]. Available: https://www.theregister.co.uk/2017/01/09/mongodb/. [Accessed: 20-Jan-2018].
[44] J. Carrie Wong and O. Solon, "Massive ransomware cyber-attack hits nearly 100 countries around the world | Technology | The Guardi," *The Guardian*, 2017.
[45] B. Hou, Y. Shi, K. Qian, and L. Tao, "Towards Analyzing MongoDB NoSQL Security and Designing Injection Defense Solution," in *Proceedings - 3rd IEEE International Conference on Big Data Security on Cloud, BigDataSecurity 2017, 3rd IEEE International Conference on High Performance and Smart Computing, HPSC 2017 and 2nd IEEE International Conference on Intelligent Data and Securit*, 2017, pp. 90–95.
[46] Verizon, "2017 Data Breach Investigations Report," 2017.
[47] Verizon, "2017 Data Breach Investigations Report Tips on Getting the Most from This Report," *Verizon Bus. J.*, no. 1, pp. 1–48, 2017.
[48] T. Moore, "On the harms arising from the Equifax data breach of 2017," *International Journal of Critical Infrastructure Protection*, vol. 19. pp. 47–48, 2017.
[49] M. Burgess, "That Yahoo data breach actually hit three billion accounts | WIRED UK," *Wired*, 2017. [Online]. Available: https://www.wired.co.uk/article/hacks-data-breaches-2017.
[50] D. Olenick, "Cyber Security - Alaska Office of Children's Services Hit With Data Breach," *SC Media*, 2017. [Online]. Available: http://www.cyber.myindustrytracker.com/en/article/71022/alaska-office-of-childrens-services-hit-with-data-breach. [Accessed: 20-Jan-2018].
[51] Desot Tom, "How criminals use Artificial Intelligence and Machine Learning," *TechNews*, 2017. [Online]. Available: https://betanews.com/2017/02/08/how-criminals-use-artificial-intelligence-and-machine-learning/. [Accessed: 20-Jan-2018].
[52] M. I. Jordan and T. M. Mitchell, "Machine learning: Trends, perspectives, and prospects," *Science*, vol. 349, no. 6245. pp. 255–260, 2015.
[53] E. Yu, "AXA Insurance data breach hits 5,400 customers in Singapore | ZDNet," *ZDnet*, 2017. [Online]. Available: http://www.zdnet.com/article/axa-insurance-data-breach-hits-5400-customers-in-singapore/. [Accessed: 20-Jan-2018].
[54] N. DuPaul, "Man in the Middle Attack: Tutorial & Examples," *VERACODE*, 2017. [Online]. Available: https://www.veracode.com/security/man-middle-attack. [Accessed: 20-Jan-2018].
[55] B. Barth, "Nearly 29M records stolen in breach of Latin American social network Taringa!," *SC Media*, 2017. [Online]. Available: https://www.scmagazine.com/nearly-29m-records-stolen-in-breach-of-latin-american-social-network-taringa/article/686421/. [Accessed: 20-Jan-2018].
[56] H. Kumar *et al.*, "Rainbow table to crack password using MD5 hashing algorithm," in *2013 IEEE Conference on Information and Communication Technologies, ICT 2013*, 2013, pp. 433–439.
[57] P. Gupta and S. Kumar, "A Comparative Analysis of SHA and MD5 Algorithm," *Int. J. Comput. Sci. Inf. Technol.*, vol. 5, no. 3, pp. 4492–4495, 2014.
[58] J. Murdock, "Taringa hacked: More than 28 million user records stolen from popular social website," *International Business Times*, 2017. [Online]. Available: http://www.ibtimes.co.uk/taringa-hacked-more-28-million-user-records-stolen-popular-social-website-1637930. [Accessed: 20-Jan-2018].