International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER SSRN

IJIEMR Transactions, online available on 11th Jan 2023. Link :http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=Issue 01

DOI: 10.48047/IJIEMR/V12/ISSUE 01/65

Title **Cybersecurity using Artificial Intelligence**

Volume 12, ISSUE 01, Pages: 686-694

Paper Authors

Surendhar Soundrarajan, Sathwika Dimmiti, Pyla Hymavathi, Thakur Tanish Singh, Vinay Kumar Ushagoni

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Cybersecurity using Artificial Intelligence

Surendhar Soundrarajan[1], Sathwika Dimmiti[2], Pyla Hymavathi[3],

Thakur TanishSingh[4], Vinay Kumar Ushagoni[5].

[1]Assistant professor, Department of Computer Science Engineering- Artificial Intelligence and Machine Learning, KG Reddy College of Engineering and Technology, Hyderabad, India. Email: s.surendhar@kgr.ac.in

[2]UG Scholar, Department of Computer Science Engineering- Artificial Intelligence and Machine Learning, KG Reddy College of Engineering and Technology, Hyderabad, India.

[3]UG Scholar, Department of Computer Science Engineering- Artificial Intelligence and Machine Learning, KG Reddy College of Engineering and Technology, Hyderabad, India.

1. [4]UG Scholar, Department of Computer Science Engineering- Artificial Intelligence and Machine Learning, KG Reddy College of Engineering and Technology, Hyderabad, India.

[5]UG Scholar, Department of Computer Science Engineering- Artificial Intelligence and Machine Learning, KG Reddy College of Engineering and Technology, Hyderabad, India

Abstract

Cryptocurrencies have recently emerged as a major digital currency,aid,and financial system some artificial intelligence techniques are necessary to reduce investment risk and forecast cost, trend, construction, and trickery detection. Recent search on the artificial intelligence techniques for Cryptocurrencies, specifically Bitcoin, (As the first independent Cryptocurrency that heavily exploits the field of cryptography for generating and verifying the transactions, Bitcoin was launched at the end of 2008.) the most well-known Cryptocurrency, is covered in the paper. The most major research with regard to Cryptocurrencies and Bitcoin, as well as several other revelent research activities, have been analyzed. Artificial intelligence and Machine Learning approaches have also been examined. Some potential research paths and possibilities for improving the result's efficiency are overlooked, lately during the recent years. Cybersecurity and artificial intelligence have developed rapidly. Its pursuit has a favourable impact on the markets, organizations, and the constitution in addition to being broadly useful in finance. It benefits the world in some aspects. Machines that are resemble humans and have sufficient intelligence have been produced as a result of artificial intelligence. A type of malware also

referred as keyloggers. Therefore, it serves as the paper's main argument. Hardware keyloggers, Unfortunately, Pose a significant threat to the privacy of system users.

Introduction

In this study, cryptocurrencies using artificial intelligence methods are surveyed. This large amount of data consists of blockchain transactions, millions of

contracts signed on various exchange websites, an overwhelming amount of tweets, posts and articles on Bitcoin and other cryptocurrencies, as well as trades performed in the blockchain and on trading online platforms. Digital currencies can

only be utilized using computers or smart phones because they only exist in digital form. Because they do not require middlemen, common digital currencies are typically the most cost effective way to exchange goods. To ease and secure trade and mining, artificial intelligence systems can learn from this vast volume of data by analyzing and identifying patterns. AI enabled cybersecurity is expected to alter the way we respond to cyber-attacks. Artificial intelligence as new technology and devices are constantly being produced,there is no all-in-one solution for protecting these devices against anonymous identities.The need to remedy network app and system vulnerabilities because of continued corporate and individual cyber-attacks are factors that will likely drive growth. the majority of websites offer a user account features that requires logging in order to access services or make purchases. Visitors must fill out sensitive data on some web forms. As a business, you require an additional security layer to operate suchsites, since it contain sensitive information and personal details.

KeyLoggers: The software thatmonitors all of the user's activity ismalware. It can snapshot as well as record keystrokes. Furthermore, it tracks onlineactivity. For example, Android, Linux, and mac can install this software. Kidlogger software, for instance, is used to take screenshot. Keyloggers are risky applications that reveal all of your most sensitive login information to hacker groupin real-time, such as our bank servers, and social media accounts. All keyloggers can be divided into two types: software based and hardware based.

Keylogger that use APIs: Your keystrokes are recorded by these keylogging program's using the keyboard API, or application programming interface. An alert is delivered to the application you currently type by the hit of the keypad, causing the typed character to show up on the screen. These notifications are intercepted by API based keylogger, who record each one as distinct event. The logs are eventually stored in a file on the system's hard drive so that the hacker may easily access them.

From-Grabbing KeyLoggers:
KeyLoggers that use forms to record data from your online forms while they are being submitted. This might be your full name, phone number, address, email, login information, or credit card info. Before your data is sent to the website, the entire procedure begins as soon as you hit the Submit or Enter button.

KeyLoggers that Use the Kernel: Kernel-based keyloggers, as the title indicates, interface with the fundamental workings of your computer's operating system and collect keystrokes as they are proposed by the kernel. It is propagated using rootkits, malicious software packages that may skip the firmware of your computer and target the hardware.

Hardware based KeyLoggers: These are tools that record keystrokes by using the keyboards internal circuits. Most of the time, they are embedded into the keyboard, but can also be purchased as either Mini- PCI card or a USB connector. But it also means that in order to get this data, hackers need to physically access the keyboard. Audio KeyLoggers: These are pretty advanced. They use sound decryption techniques to capture your keystrokes at the hardware level. But this takes a lot of time, and the outcomes might not be as accurate as with other keylogger types.

Literature Review
The approach of protecting personal computers, electronic components, mobile phones, platforms, and information from dangerous attacks can be summed up to cybersecurity. App security, interconnection security, practical security, also information security are several categories of cyber security. Cyberattacks, cyberterrorism, and cybercrime all constitute cyberthreats. The phrase "Central Bank Digital Currencies"

also known as CBDC can be used to describe digital cryptocurrencies that are issued by monetary authorities. They are correlated tothe value of the physical cash used in that nation.

Numerous nations are investigating the potential impact about CBDC on their current federal systems, economies, and stability. Nine nations have fully implemented Central Bank Digital Currencies. The first nation to establish a CBDC is Africa.

Khokha Project by South Africa: The project khokha report was released by the South Africa Reserve Bank.Project khokha is really a proof of concept intended to mimic a "real-world" Experiment of a retail payment scheme based on distributed ledger technology. The project main goal was to give participants hands-on experience with various aspects of deploying DLT in a practical testing environment using various deployment methods. The project was started in January 2021 as a part of South Africa Reserve Bank. These initiatives made use of distributed ledger and blockchain technologies. Currently, Deloitte and Acenture are working on the projects centered on CBDC that is similar to projectKhokha 2.

UBIN Project by Singapore: Project Ubin is an industry led initiative to investigate the use of distributed ledger technology and blockchain for settlement

and clearing payment securities, the initiatives tries to support the monetary authorities of Singapore. When the monetary authorities of Singapore also known as MAS announced collaboration with R3 and a group of financial institutions in November 2016, the journey officially began.

STELLA Project European Central Bank: Project Stella studied how distributed ledger technology can be applied to the infrastructure of the financial markets. According to research done bycentral financial institutions and market infrastructures have the ability to power up the security and performance of existing systems. Project Stella collaborative research initiative from Central bank of Europe and the Japanese central bank, has participated in the ongoing argument since its launch in December 2016 via experimental work and theories evaluating the benefits and drawbacks.

KRONA Project By Switzerland: Krona is referred as "Central Bank Digital Currency", which is an evolution of crypto assets as it is backed by the government. It is based on smart contracts, which ensure the privacy of transactions and the users identity, much like other digital currencies.

The central bank believes that the introduction of a digital krona could improve the payment systems stability. In the event that perhaps the banking or credit company systems are drastically impacted, having access to a backup payment method is crucial. The first approved and regulated issue of the krona coin is on ekrona.com this aims to provide people all over the world with a properly secured and regulated way t purchase and trade virtual currency based on krona.

INTHANON Project by Thailand: Project Inthanon is a collaborative effort between both the bank of Thailand also known as BOT and hong Kong monetary authority also known as HKMA and explores the use of distributed ledger technology to improve theeffectiveness of cross-bencher fund transfers. In 2018 the BOT established Project Inthanon, for creating a digital currency, modifying the central bank, and promoting the ecosystem for technologytransformation.

Problem Statement

"Cyber Attacks in Digital Currency". Central bank digital currencies (CBDC) arebecoming more popular. They have the potential to build way in financial and payment efficiency.Central banks must set

the seal on their cybersecurity to ensure CBDC trust. With G7 officials not long-agovalidated principles for the CBDC and more than eighty countries are introducing some or the other design of CBDC, is a virtual money of reserve bank money that is available to society; it actually consists of personal and livelihood who have a way into savings accounts and transactions with their god country's federal bank. For reference the Bahamas, China and also Nigeria all had enacted to early CBDC programming with much to follow. Central Bank Digital Currency could help policymakers achieve goals such as payment and banking competitiveness, payment efficiency, and financial inclusions, access to secure federal bank capital in the age of virtual currency modeand also it was successful.

However, CBDC, like other virtual currency mode system, is weak for cyber security attacks, theft counterfeiting, account, and data breaches, and added to it distant challenges related to quantum computing

Citizens must be confident in the security of CBDC before they can adopt it. However, it might not a successful unless careful consideration and investment in a strong cybersecurity strategy. Cybersecurity finest standards, like those presented by the United State National Institute of Standards and Technology also known as NIST and

Microsoft STRIDE copy should be considered by decision makers.

1. Research Aims and Objectives

- To encourage the development in cyberdefence law jurisprudence.
- To take part in a range of research- based activities that look at contemporary legal developments pertaining to the development of Cyber Security law.
- To participate in exercises that create capacity in order to raise awareness of the legal aspects of cyber security law.
- Collaborating with other international groups to build a powerful suite for the sharing of knowledge, information, and best practices with regard to international cyber security to the appropriate parties.

2. Research Significance

The findings of the research paper will investigate whether it is possible to implement an AI-based cybersecurity system or algorithm with the goal of reducing cyberattacks. In order to reduce

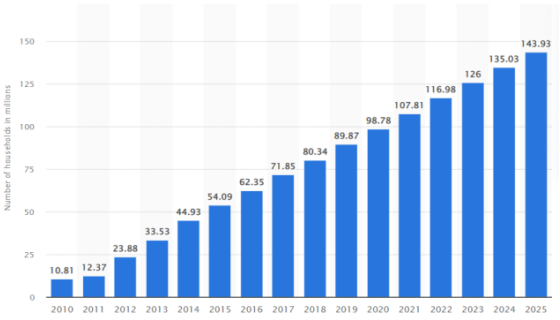
the total number of cybercrimes that the cybersecurity team must deal with, the research paper can encourage and promote the use of the proposed system in order to assist in the handling of more minor and simpler cybercrimes.

Finally, new researchers can learn more about cybersecurity from this research paper as a starting point. It is efficient and will enhance the researchers understanding of cybercrimes in an efficient manner.

3. Methodology

In terms of methodology, this study will search several groups using qualitative and quantitative methods. A qualitative approach should be employed to gather information on the number of individuals

affected by the cybercrimes. In the quantitative approach.



(Fig-1 Number of internet households in millions)

Windows has created a framework for the thread modelling to up the security risks. data manipulation inside a network to archive the harmful objective to protect users' personal information. Process for Attack Simulation and threat Analysis, this is a dynamic threat identification developed by using the attacker centric view. The user should change their passwords frequently and use all the possible ways to secure a strong password to save them from the attackers.

4. Overview of the Proposed System

The number of cybercrime cases is increasing. which means that more resources are needed to prevent and address these crimes. its vital to remember that cybercrimes and are almost always performed and occasionally, attacks may even occur every hour or few minutes. Whereas the threat is persistent. Its also crucial to remember that those in charge ofdealing with cybercrimes are not always available to stop it. A cybersecurity team must work extremely hard to maintain full operations every single day of the week.

Algorithm 1:

Bot Detection Algorithm using Spearman's Rank Correlation (SRC)

if KeyboardState function(s) is executed (i.e.keyloggingactivity)then

If SRC[KeyboardState,CommFunc]>Threshold and [KeyboardState,FileAccess]>Threshold then Strong detection else if SRC[KeyboardState,CommFunc]Thresh old) then Weak detection else if(SRC[KeyboardState,CommFunc]Threshold) or (SRC[KeyboardState,CommFunc]> Threshold and SRC[KeyboardState,FileAccess]<Threshold) then Normal detection else

(Fig-4 Bot Detection algorithm)

The proposed method aims to relieve the cybersecurity team's workload and resolve simpler problems using AI Machine Learning.

Bot is a program that was unknowingly placed on a user's computer. As a method of communication, the malware uses the attackers IRC (internet relay chat) network.The program reacts to commands given by attacker. By the advantage of well-known flaws in the OS and other software, a bot travels to additional hosts. The user's computer can become infected in several ways, including through emails, worms, and viruses. The way that this software spread is by sending additional emails to other computers are impacted by this. To join the channel, bot makes a connection to IRC server. The bot either runs default commands or waits for commands from botmaster, through the IRC protocol, the botmaster and bot talk to one another. The flexibility of the IRC protocol is a benefit.

This algorithm is benefits include altering users to existence of bot software with in the allotted time frame. It keeps track of different bot pattern behaviour. It can successfully identify a single bot. The bot identification process used by this programis based on Keylogging activities. With a predetermined time limit, it effectively finds a single bot. If the controller waits for a random amount of time before performing the task, the algorithm is unable to identifyit, Resulting in a poor detection choice.

Technologies used Artificial Intelligence, Cyber Security, Blockchain, Machine Learning.

Conclusion

This research paper's conclusion aims to provide light on the interconnected issues of rising cybercrimes, staffing shortages, and burnout in the cybersecurity industry. This might demonstrate the necessity of an AI-based Cybersecurity system to decreasethe overall number of cybercrime instances encountered either by the cybersecurity team or to offer the customer minimal protection by behavior principles known as cybercrimes from occurring. It would makeeveryone's use of the web safer.

References

[1] Detecting Bots Based on Keylogging Activities Yousof Al-Hammadi and Uwe Aickelin Department of Computer Science and Information Technology, TheUniversity of Nottingham.

[2] International Journal of Innovative Research in Science, Engineering and

Technology (An ISO 3297: 2007 CertifiedOrganization) Vol. 5, Issue 5, May 2016Copyright to IJIRSET DOI:10.15680/IJIRSET.2016.0505159 7542 Unprivileged Detection of User SpaceKeyloggers Mugdha Kolte1, Rutuja Wadekar2 , Rachana Late3 , Palak lodha4Saranga Bhutada5 B.E.Student,Department of Information Technology, MITCOE, Kothrud, Pune, India1 B.E.Student, Department of Information Technology, MITCOE, Kothrud, Pune,India2 B.E. Student, Department of Information Technology, MITCOE, Kothrud, Pune, India3 B.E.Student,Department of Information Technology, MITCOE, Kothrud, Pune, India4 Assistant Professor, Department of Information Technology, MITCOE, Kothrud, Pune,India5

[3] Review AI-based Cybersecurity : A solution to the emerging cybercrimes threat Wong Jing Tian

[4] "Keyloggers in Cybersecurity Education," Christopher A. Wood, Rajendra K. Raj, In Proceeding of the 2010 International Conference on Security and Management, pp. 293-299, July 12-15,2010

[5] Keyloggers Software Detection Techniques A.Solairaj1 , S.C.Prabanand2, J.Mathalairaj3, C.Prathap4 and L.S.Vignesh5 Assistant Professor 1, 2,3,4,5, Nadar Saraswathi College of Engineering and Technology.