STRUCTURING CYBERSECURITY CONCLAVE

NITYASH SOLANKI
Ph.D. Candidate & Founder of "ONSHI", Department of Law, Jagannath University
Email ID: nityashsolanki@gmail.com

Abstract
There has been a dramatic shift from the traditional to the smart grid in recent years. A smart grid is only one example of how innovation can have its drawbacks. Safeguarding the smart grid against possible hackers is one of its biggest difficulties. The largest problem is maintaining such a massive network, as millions of sensors are constantly transmitting and receiving data packets over it. The availability, confidentiality, and integrity of the smart grid are crucial components that can be compromised by any cyberattack. cyberattacks can affect any level of the smart grid network, including customers using the network, smart devices and sensors communicating with one another, and decision makers overseeing the network. The smart grid network's cybersecurity from every angle has been looked upon, identifying potential risks and weaknesses and outlining three tiers of protection to keep them at bay.
***Keywords**: Cybersecurity, Cryptocurrency, AI, Block chain, zero trust security, cyberattack.*

INTRODUCTION

Information sharing and other professional activities such as business, shopping, banking, ads, services, etc. have all become ubiquitous in today's globe through cyber civilization. As the number of people using the internet continues to skyrocket, so too has the number of cybercrimes. The widespread and excessive use of web apps has been the primary driver of this growth. Cybercriminals are able to obtain unauthorized access to systems by taking advantage of design flaws in these web apps[1]. As a result, cyber security has risen to the forefront of academic and professional agendas[2].
One definition of cyber security is "the set of procedures, policies, measures, guidelines, actions, training, good practices, assurances, and technologies that are available for use in protecting information systems and the assets of their users from harm in cyberspace" [3]. Detecting, preventing, and responding to cyber assaults is what cyber security is all about, and it's something that everyone is interested in and concerned about these days[4].
Many studies have examined different forms of security breaches in diverse cyber settings, each with its own oddities. Following literature suggests several cyber security risk identification and mitigation approaches. But obtaining the current research is required before continuing in this sector. This research is an effort to fill the gap and to seek a complete picture of cyber security vulnerabilities and solutions.

CYBER SECURITY

According to one definition, security is "the protection against undesirable disclosure, destruction, or modification of data in a system and also the protection of systems themselves."[5]. If you believe ISACA (Information Systems Audit and Control Association), "Cyber security is concerned with the security and privacy of digital assets—everything from networks to computing devices and information

[1] Lun, Y.Z.; et al.: Cyber-physical systems security: a systematic mapping study. arXiv:1605.09641 (2016)
[2] Razzaq, A.; et al.: Cyber security: threats, reasons, challenges, methodologies and state of the art solutions for industrial applications. In: 2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS). IEEE (2013)
[3] Von Solms, R.; Van Niekerk, J.: From information security to cyber security. Comput. Secur. 38, 97–102 (2013)
[4] Benson, V.; McAlaney, J.; Frumkin, L.A.: Emerging threats for the human element and countermeasures in current cyber security landscape. Psychological and Behavioral Examinations in Cyber Security, pp. 266–271. IGI Global, Hershey (2018)
[5] Valeriano, B.; Maness, R.C.: International relations theory and cyber security. In: Brown, C., Eckersley, R. (eds.) The Oxford Handbook of International Political Theory, p. 259. Oxford University Press, Oxford (2018)

that is processed, stored or exchanged by internetworked information systems"[6] is true. When it comes to protecting user assets and cyber organizations, the International Telecommunications Union defines cyber security as a combination of rules, regulations, best practices, and methodologies[7]. Protecting computer systems from intrusion and assaults is the definition of cyber security according to the Merriam-Webster dictionary[8]. To prevent malicious actors from gaining access to computer systems and networks through the Internet, cyber security measures are put in place.

Cyber security researchers employ different terms, as illustrated in these definitions. Many cyber security aspects have been defined. Some definitions emphasize privacy and security, while others emphasize the need for data availability, confidentiality, and integrity policies. Other academics stressed the need for computer security processes and technology. Cyber security protects valuable assets from unwanted access. Equally essential, these definitions emphasize cyber security.

CRYPTOCURRENCIES USING BLOCKCHAIN FOR E-COMMERCE ONLINE PAYMENT

When people buy and sell things online, it's called e-commerce. New technologies have greatly simplified, secured, and elevated the level of e-commerce, which is practiced all over the globe. Electronic wallets, credit/debit cards, direct debit, electronic funds transfers, smart cards, and cryptocurrency are just a few of the many online payment methods accepted in e-commerce[9]. Since blockchain technology and cryptocurrency are still in their early stages, they are finding widespread use.

Banks and financial institutions are investigating payments, asset registries, regulatory reporting, know-your-customer, digital currency exchange, digital security experimentation, gifts, and more. Financial institutions like ANZ[10] (Australia and New Zealand Banking Group Limited), Citi[11], BNP[12] (Banque Nationale de Paris), EBA[13] (European Banking Authority), Deutsche Bank, NASDAQ[14] (National Association of Securities Dealers Automated Quotations), and DBS[15] (Development Bank of Singapore Limited) are investigating Blockchain technology[16].

CORPORATE GIANTS SHIFTING FROM LEGAL TENDER TO CRYPTOCURRENCIES

One late 2022 estimate found 2,352 US firms accepting bitcoin, not including bitcoin ATMs. Bitcoin and other crypto and digital assets are being used by more companies globally for investment, operational, and transactional purposes. A survey of 2,000 senior executives at US consumer businesses found that merchants are adopting digital currency payments to gain a competitive edge and to expand the use of digital currency.[17] Big brands accept bitcoin for groceries and airline tickets. Some sports clubs and groups are accepting cryptocurrencies and considering NFTs to enhance fan immersion. More stores are embracing bitcoin to attract bitcoin-paying customers. Even real estate

[6] von Solms, B.; von Solms, R.: Cybersecurity and information security—what goes where? Inf. Comput. Secur. 26(1), 2–9 (2018)

[7] Ron, M.: Situational status of global cybersecurity and cyber defense according to global indicators. Adaptation of a model for ecuador. In: Developments and Advances in Defense and Security: Proceedings of the Multidisciplinary International Conference of Research Applied to Defense and Security (MICRADS 2018). Springer (2018)

[8] Al Mazari, A.; et al.: Cyber terrorism taxonomies: defnition, targets, patterns, risk factors, and mitigation strategies. Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications, pp. 608–621. IGI Global, Hershey (2018)

[9] "4.1 Electronic Payment Systems (EPS)". n.d. Available from: http://ocw.metu.edu.tr/pluginfile.php/354/mod_resource/content/0/Lecture_4.pdf.

[10] Australia and New Zealand Banking Group Limited

[11] Citi Bank

[12] Banque Nationale de Paris

[13] European Banking Authority

[14] National Association of Securities Dealers Automated Quotations

[15] Development Bank of Singapore Limited

[16] "Know more about Blockchain: Overview, Technology, Application Areas and Use Cases" 2018. MEDICI, Available from: https://gomedici.com/an-overview-of-Blockchain-technology.

[17] Claudina Castro Tanco, Merchants getting ready for crypto: Merchant Adoption of Digital Currency Payments Survey, Deloitte, 2022.

can be bought with bitcoin. A number of well-known corporations have invested millions in bitcoin. Crypto and digital assets are being used in commercial and investment applications.[18]
Business using bitcoin brings many potentials and obstacles. Any new frontier has great temptations and unexpected risks. That's why organizations considering embracing crypto should have a clear reason and a list of questions.

CRYPTOCURRENCY AND AI

As AI automates, streamlines, and improves the bitcoin industry, traders, investors, and blockchain developers can benefit from its insights and tools. Deep-learning algorithms can help investors and traders analyze the market and make trading decisions. Algorithms can optimize mining settings for productivity and profitability in cryptocurrency mining. In automated trade execution, trend prediction, and data analysis, algorithms are used. AI partners well in security. Decentralized systems and hardware wallets for digital assets can be secured and detect suspicious transactions. Finally, AI cryptocurrencies are gaining popularity: AI blockchain platforms like The Graph[19], SingularityNET[20], and Fetch.ai[21] use these currency.
A number of cryptocurrency initiatives have taken use of the established link between AI and international trade to falsely market their wares as "elf-adjusting tokens through algorithms," also called algorithmic stablecoins. Do Kwon, a software entrepreneur from South Korea, is a prime example. Algorithmic stablecoin Luna was introduced with the bold assertion that it could regulate token values and fix trade volumes automatically. Unfortunately, investors lost a lot of money since Luna was an incomplete and unrealistically hopeful project, and Do Kwon was arrested because of it. Also, malicious actors could try to find weak spots in the AI systems that are employed to analyze or secure cryptocurrencies. The bitcoin ecosystem is vulnerable to these and related threats to its fairness, security, and integrity.[22]

ZERO TRUST SECURITY

A common definition of the Zero Trust Model is trust between all parties, including people, devices, networks, and other variables inside and outside an organization's network. It considers internal and external risks to reduce vulnerable systems and prevent unwanted access to critical network data, according to research.[23]
Cybersecurity used to be "trust but verify." Companies assumed users and devices were trusted by default and only validated their identities and permissions after they acquired network access. Modern cyberattacks render this model ineffective. Cyberattacks are becoming more sophisticated and focused. Hackers now go beyond stealing data from networks. They are now seeking ways to manage systems and networks and steal sensitive data. Zero trust security protects your company against cyberattacks better. Zero trust security makes it harder for attackers to access your systems and networks by thinking no user or device can be trusted. The future of cybersecurity is zero trust. By using zero trust security, you can safeguard your company from contemporary threats. Learn about zero trust security and consider implementing it in your organization if you haven't previously.

[18] Kathleen Marshall, “Fidelity to start offering bitcoin and ether trading,” Investopedia, November 3, 2022.
[19] https://thegraph.com/
[20] https://singularitynet.io/
[21] https://fetch.ai/
[22] Ramanpreet Kaur, Dušan Gabrijelčič, Tomaž Klobučar, Artificial intelligence for cybersecurity: Literature review and future research directions, Information Fusion, Volume 97, 2023, 101804, ISSN 1566-2535,
https://doi.org/10.1016/j.inffus.2023.101804.
(https://www.sciencedirect.com/science/article/pii/S1566253523001136)
[23] Z. Zaheer, H. Chang, S. Mukherjee, and J. Van Der Merwe, “EZTrust: Network-Independent Zero-Trust Perimeterization for Microservices,” 2019, doi: 10.1145/3314148.3314349.

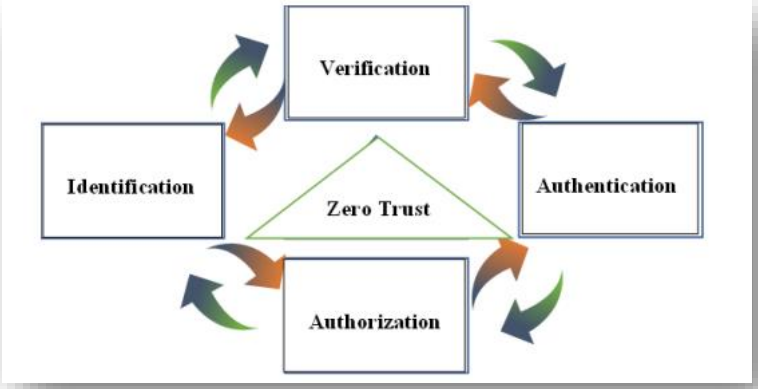

Figure 1: Zero trust drivers[24]

CASES

Over 30,000 US businesses were hit by a massive cyberattack on Microsoft Exchange[25], one of the world's largest email services. The hackers used four zero-day vulnerabilities to access small business and local government emails. Microsoft patched the flaws, but if server owners didn't update, attackers might exploit them again. Microsoft couldn't patch the systems instantly because they weren't cloud-based. Microsoft patched the flaws, but if server owners didn't update, attackers might exploit them again. Microsoft couldn't patch the systems instantly because they weren't cloud-based. Facebook[26], one of the world's largest companies, has leaked data and caused uproar. After going public in 2012, Facebook has continuously grappled with data breaches. The company's greatest data breach in April 2021 exposed around 530 million people's identities, phone numbers, account names, and passwords. Facebook disclosed a weakness in its contact sync tool that allowed hackers to scrape user profiles for customer data. Although Facebook claimed no data was hacked or misused, it's impossible to verify since the information remained available for a brief time. With names, phone numbers, and emails, hackers and scammers can easily exploit unwary people.

SOLUTIONS

Solutions are either technical or nontechnical. Physical and administrative solutions are nontechnical. Area protection, computing device physical security, data center disaster recovery strategy, and backup location are critical to physical security. Administrative management and changes are also crucial to nontechnical solutions. Dealing with cyber threats also requires policies, procedures, standards, risk assessment, vendor management, assigned duties, and training. Cybersecurity experts can develop the strongest protection system, but untrained users will not give enough security. So non-technical solutions are as vital as technological ones. Technologies and platforms, tools, and AI/data science are technical solutions. Figure 2 shows major technologies and platforms. Cryptography secures disk and transit data. Access control reduces remote attack and privilege escalation by restricting data access. Big data analysis reveals unknown trends and malicious attack features.

The evolution of attack surfaces and techniques reduces the effectiveness and practicality of present detection systems. Add new solutions or create new mechanisms to fight smarter attacks. This can be done with statistics, probability, datamining, and machine learning. The scientific method of statistics examines, evaluates, and reveals patterns in data. The probability technique determines the likelihood of an event occurring. Data mining finds and extracts patterns from massive databases. It affects statistics, machine learning, and CS. Machine learning lets computers learn without programming. The data is described algorithmically via ML. Cyber security has long leveraged statistics and probability. Recently, data mining and ML have become prominent in cyber security[27].

[24] S. Tyagi, "7 Key Tenets of Zero Trust Architecture," Colortokens, 2021. https://colortokens.com/blog/key-tenets-zero-trustarchitecture/.

[25] Microsoft Exchange Server data breach (2021)

[26] 2021 Facebook leak

[27] Houichi, M.; Jaidi, F.; Bouhoula, A. A Systematic Approach for IoT Cyber-Attacks Detection in Smart Cities Using Machine Learning Techniques. In Proceedings of the International Conference on

Existing attack detection systems gain new characteristics from data mining and ML. These novel technologies also improve cyber attack detection systems.

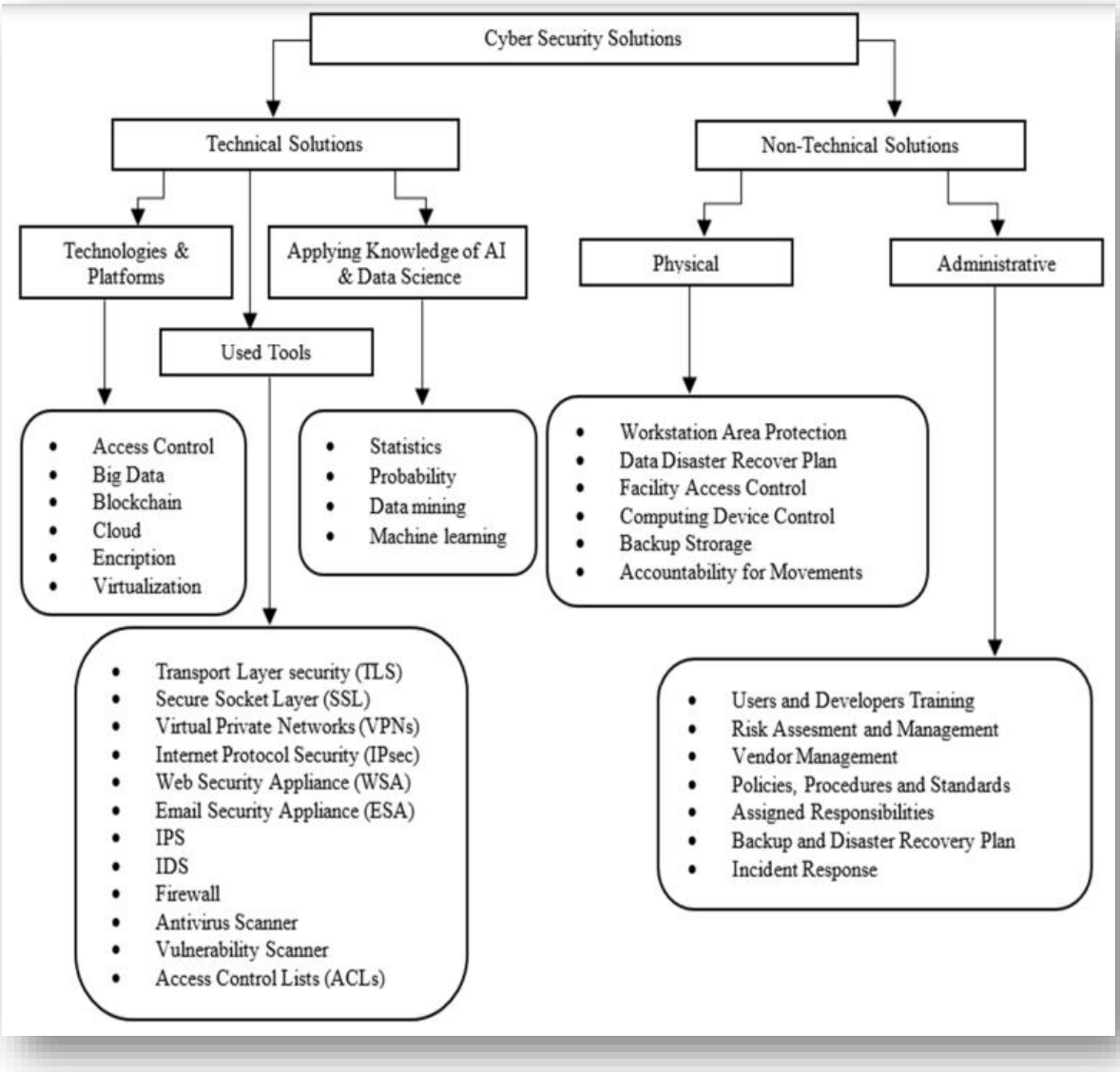

Figure 2: Represent the technical and non-technical cyber security solutions.

CONCLUSION

The allure of e-commerce for contemporary organisations is counterbalanced by the perilous cyber security concerns it faces. Although organisations allocate significant resources to tackle the problem, it remains challenging. Cyberattacks specifically aim to compromise both personal and organisational data. Technology provides novel approaches for conducting business and numerous advantages, although the presence of cyber security risks is inevitable. Investing in e-commerce security is essential for gaining a competitive edge and achieving success in business. It is imperative to avoid compromising clients' trust by exposing their data. Stringent monitoring procedures are necessary to address organisational and customer mistakes. Examples include using robust passwords and exercising caution when clicking on links or downloading files. It is imperative to exercise prudence and allocate resources towards implementing robust e-commerce technology.

Advanced Information Networking and Applications, Toronto, ON, Canada, 12–14 May 2021; pp. 215–228.

REFERENCES

[1] Lun, Y.Z.; et al.: Cyber-physical systems security: a systematic mapping study. arXiv:1605.09641 (2016)

[2] Razzaq, A.; et al.: Cyber security: threats, reasons, challenges, methodologies and state of the art solutions for industrial applications. In: 2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS). IEEE (2013)

[3] Von Solms, R.; Van Niekerk, J.: From information security to cyber security. Comput. Secur. 38, 97–102 (2013)

[4] Benson, V.; McAlaney, J.; Frumkin, L.A.: Emerging threats for the human element and countermeasures in current cyber security landscape. Psychological and Behavioral Examinations in Cyber Security, pp. 266–271. IGI Global, Hershey (2018)

[5] Floyd, D.H.; Shelton, J.W.; Bush, J.E.: Systems and methods for detecting a security breach in an aircraft network. Google Patents (2018)

[6] Valeriano, B.; Maness, R.C.: International relations theory and cyber security. In: Brown, C., Eckersley, R. (eds.) The Oxford Handbook of International Political Theory, p. 259. Oxford University Press, Oxford (2018)

[7] von Solms, B.; von Solms, R.: Cybersecurity and information security—what goes where? Inf. Comput. Secur. 26(1), 2–9 (2018)

[8] Ron, M.: Situational status of global cybersecurity and cyber defense according to global indicators. Adaptation of a model for ecuador. In: Developments and Advances in Defense and Security: Proceedings of the Multidisciplinary International Conference of Research Applied to Defense and Security (MICRADS 2018). Springer (2018)

[9] Al Mazari, A.; et al.: Cyber terrorism taxonomies: defnition, targets, patterns, risk factors, and mitigation strategies. Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications, pp. 608–621. IGI Global, Hershey (2018)

[10] "4.1 Electronic Payment Systems (EPS)". n.d. Available from: http://ocw.metu.edu.tr/pluginfile.php/354/mod_resource/content/0/Lecture_4.pdf.

[11] "Know more about Blockchain: Overview, Technology, Application Areas and Use Cases" 2018. MEDICI, Available from: https://gomedici.com/an-overview-of-Blockchain-technology.

[12] Ramanpreet Kaur, Dušan Gabrijelčič, Tomaž Klobučar, Artificial intelligence for cybersecurity: Literature review and future research directions, Information Fusion, Volume 97, 2023, 101804, ISSN 1566-2535,https://doi.org/10.1016/j.inffus.2023.101804.(https://www.sciencedirect.com/science/article/pii/S1566253523001136)

[13] J. Petters, "What is Zero Trust? A Security Model," Inside Out Security Blog, 2021. https://www.varonis.com/blog/what-is-zerotrust

[14] L. Odell, B. Farrar-Folley, C. Fauntleroy, and R. Wagner, "In-Use and Emerging Disruptive Technology Trend," Inst. Def. Anal., 2015.

[15] Claudina Castro Tanco, Merchants getting ready for crypto: Merchant Adoption of Digital Currency Payments Survey, Deloitte, 2022.

[16] Kathleen Marshall, "Fidelity to start offering bitcoin and ether trading," Investopedia, November 3, 2022.

[17] Z. Zaheer, H. Chang, S. Mukherjee, and J. Van Der Merwe, "EZTrust: Network-Independent Zero-Trust Perimeterization for Microservices," 2019, doi: 10.1145/3314148.3314349.

[18] S. Tyagi, "7 Key Tenets of Zero Trust Architecture," Colortokens, 2021. https://colortokens.com/blog/key-tenets-zero-trustarchitecture/.

[19] Houichi, M.; Jaidi, F.; Bouhoula, A. A Systematic Approach for IoT Cyber-Attacks Detection in Smart Cities Using Machine Learning Techniques. In Proceedings of the International Conference on Advanced Information Networking and Applications, Toronto, ON, Canada, 12–14 May 2021; pp. 215–228.