International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

A Cumulation of the Cyber Security Vulnerabilities in Latest Technologies

Karan Chawla

Ashoka University

Abstract: ***Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. Different kinds of cyber attacks include Malware, Ransomware, Distributed denial of service (DDoS) attacks, Spam and Phishing, Corporate Account Takeover (CATO), Automated Teller Machine (ATM) Cash Out. Cybersecurity is a must in the digital age. Millions of people's personal information may be exposed as a result of a single security breach. These violations have a negative financial impact on the businesses as well as a loss of client confidence. Therefore, it is crucial to have cyber security to shield both persons and businesses from spammers and online crooks. This paper reviews information about the latest methodologies used to defend against potential cyber attacks in the latest technologies, critiques the current methods and provides references for future works. The review paper is a cumulation of Artificial Intelligence based detection models for cybersecurity threat analysis for modern day systems. A systematic search was performed on various electronic databases (SCOPUS, Science Direct, IEEE Xplore, Web of Science, ACM, and MDPI). This Review paper discusses artificial intelligence based detection methods for cyber threat analysis for modern day systems which include, cloud computing, connected and automated vehicles (CAVs) which include CAN (Controller Area Network) Buses, Internet of Things (IOT), Fintech (Financial Technology), Vehicle to Infrastructure Applications. The drawbacks of the three technologies under review have been underlined in the conclusion and are further explained using particular statistics. Some of the problems mentioned include the lack of adequate testing done by the manufacturers when the software is deployed in the context of smart cities. There is little to no overlap in the methodologies utilized for any of the aforementioned technologies, such as gradient boost in CAVs, and each has its own literature. There aren't enough datasets and, consequently, detection algorithms because the majority of research only addresses theoretical difficulties. Finding methods to apply a methodology from system 1 to system 2 or vice versa is one strategy to improve efficiency or wiser development.***

Keywords: Cyber security, cyber attacks, detection models, Connected and Automated Vehicles, IOT, Smart City, detection algorithms, cyber security protections

1. Introduction

The main goal of the modern cyber security sector is to defend systems and devices from intruders. While it can be challenging to picture the bits and bytes driving these efforts, it is much simpler to think about the outcomes. Without the diligent efforts of cyber security experts, it would be almost impossible to use many websites due to ongoing attempts at denial-of-service attacks.

It would be simple to take out modern necessities like the electricity grids and water treatment facilities that keep the world functioning smoothly without strong cyber security protections.

Cybersecurity is crucial because it protects the way of life that we have grown accustomed to.

The most expensive and rapidly expanding type of cybercrime is information theft. caused mostly by the expansion of identity information vulnerability on the web through cloud services.

However, it is not the only one. Power grids and other infrastructure are managed by industrial controls, which can be destroyed or disturbed. Cyberattacks may also seek to compromise data integrity (damage or change data) in order to sow discord within a company or government, so that identity theft isn't their main objective.

Cybercriminals are evolving as they gain experience, changing the targets they choose, the ways in which they impact businesses, and the ways in which they attack various security systems.

Ransomware, phishing, and spyware are still the easiest ways to enter a computer system, but social engineering is still the most straightforward method. Another frequent attack vector is third-and fourth-party suppliers who handle your data and have subpar cybersecurity procedures, which emphasizes the significance of vendor risk management and third-party risk management. The average cost of cybercrime for an enterprise has climbed by $1.4 million over the past year to $13.0 million, and the average number of data breaches has increased by 11% to 145, according to Accenture and the Ponemon Institute's Ninth Annual Cost of Cybercrime Study. The need for information risk management has never been greater.

Lack of attention to cybersecurity can harm your company in a number of ways, including:

- Financial Costs-Intellectual property theft, business information theft, commercial interruption, and the cost of fixing broken systems.
- Cost of Reputation-customers to competitors, a decline in consumer confidence, and negative media coverage.
- Regulational Fees-Cyber Crimes may result in regulatory fines or sanctions for your firm because of GDPR and other data breach legislation.

Regardless of size, all firms must make sure that all employees are aware of cybersecurity hazards and how to counter them. Regular training and a working structure that

attempts to lower the risk of data leaks or breaches should be part of this. It is challenging to comprehend the direct and indirect consequences of many security breaches given the nature of cybercrime and how challenging it may be to detect. This is not to say that even a little data breach or other security incident won't cause significant reputational harm. Customers actually anticipate more advanced cybersecurity safeguards as time goes on.

Connected and Automated Vehicles (CAVs) [1]

It is believed that CAVs will be on the road for commercial uses as early as 2025. However, issues in CAV cyber security have not been considered as much as other CAV technologies, thus being of increasingly critical importance and high priority in current CAV developments. Cyber-attacks in CAVs may cause serious consequences, not only relating to the leakage of personal information but also to physical injuries or even fatalities.

CAV technologies are becoming more advanced and mature now. It is believed that CAVs will be on the road for commercial uses as early as 2025. However, issues in CAV cyber security have not been considered as much as other CAV technologies, thus being of increasingly critical importance and high priority in current CAV developments. Cyber-attacks in CAVs may cause serious consequences, not only relating to the leakage of personal information but also to physical injuries or even fatalities.

CAVs (Connected and Automated Vehicles) use data from other vehicles or infrastructure within the network to operate. The vehicles are fully automated, which means that they do not require user input to conduct operations.

The society of automotive engineers declares six layers of automation for vehicles, capability to conduct simultaneously longitudinal or lateral driving tasks, the capability for objects and events detection and response, the capability of recovery when a system failure happens and the limitation of the operational design domain. At each different automation level, the duty of the driver and the CAV system differs.

This paper looks at removing the elements not associated with CAV and removes them from the KDD99 dataset to create a new data set called KDD. It has created two algorithms demonstrated on Unified Model Language (a visual language), Decision Tree and Naive Bayes. The two models are compared by the parameters of precision, timing and accuracy.

Most research has only focused on single specific attacks like location spoofing or adversarial attacks specific to algorithms. There is a lack of datasets as most research only focuses on theoretical aspects and subsequently there is a lack of detection methods.

In CAVs, Vehicle Data is the most fundamental element in a UML diagram,

Decision Tree is one of the most-used classification models, with good readability [55]. It is one of the classification models structured as a tree of nodes and branches connected by one-directional edges. Each internal node of the Decision Tree (with branches leading to child nodes) represents a decision variable with respect to an attribute, while each branch represents a decision taken on the attribute, leading to the child nodes of different attribute values. The leaves of the tree (with no branches and child nodes) represent the classification.

The C4.5 technique is used in weka on the KDD99 data set for the Decision Tree model. C4.5 conducts the classification by calculating the information gain ratio of each attribute, and chooses attributes with the biggest information gain ratio as the root node.

$$\text{Entropy}(V) = -\sum i = 1 npi \cdot \log(pi)$$

It can be seen that both machine learning classification models had high accuracy when identifying CAV cyber-attacks. The false positive rates were low in all the attack data. When identifying the PROBE attacks, Naive Bayes performed excellently, while Decision Tree did not perform as well when detecting the ipsweep attacks. When identifying the DoS attacks, both models performed similarly; while, when detecting the pod attacks, the accuracy of Decision Tree was much higher. Both models performed poorly under the U2R and R2L attacks, due to the limited number of records of the U2R and R2L attacks in the training data sets. However, it can be seen that Naive Bayes still successfully detected 2.3% guess_passwd attacks, the accuracy of which was slightly higher than that of the Decision Tree model.

It is noticeable that both machine learning algorithms performed poorly on attack types which were only included in the testing data set; namely mailbomb, udpstorm, **httptunnel**, worm and xsnoop. The accuracy of identifying these five attack types were all zero, meaning none of them were detected. This is due to the fact that both Decision Tree and Naive Bayes build models using supervised learning and, thus, are not able to detect unseen new attack types. Further investigations on building classification models or clustering models on unseen types of attacks remain an interesting work for our future research.

IOT[2]

The large-scale growth of the Internet of things (IoT) in recent years has contributed to a significant increase in fog computing, smart cities, and Industry 4.0, all of which execute the complex data processing of confidential information that must be protected against cybersecurity attacks. Cybersecurity attacks have increased rapidly in

[1] He, Qiyi, Xiaolin Meng, Rong Qu, and Ruijie Xi. "Mathematics | Free Full-Text | Machine Learning-Based Detection for Cyber Security Attacks on Connected and Autonomous Vehicles." *MDPI*, Multidisciplinary Digital Publishing Institute, https://www.mdpi.com/2227-7390/8/8/1311. Accessed 24 Jan. 2023.

[2] Abdullahi, Mujaheed, et al. "Detecting Cybersecurity Attacks in the Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review." *MDPI*, Multidisciplinary Digital Publishing Institute, 10 Jan. 2022, www.mdpi.com/2079-9292/11/2/198.

various domains, such as smart homes, healthcare, energy, agriculture, automation, and industrial processes [1]. As a result of their wide range of services, IoT device sensors generate large amounts of data that requires authentication, security, and privacy. Previously, traditional methods and frameworks were used to ensure the security of IoT. However, the application of different artificial intelligence (AI) methods for detecting cybersecurity attacks has gained in popularity over the years.

Support Vector Machines, Random Forest, Xtreme Gradient Boosting (XGBoost), Neural Networks, Recurrent Neural Networks are the most used detection based systems used to tackle cybersecurity issues in IOT.

Certain limitations exist because the use of AI in cybersecurity detection introduces considerable exposure to IoT devices and networks. In addition to the development of IoT, several centralized attack detection mechanisms have been proposed to detect attacks in the IoT using a supervised ML algorithm. In spite of this, these mechanisms have failed to achieve significant results because of the distinct requirements of devices, such as scalability and distribution. However, there's a need for IoT security guidelines to evaluate the existing methods. Previous systematic reviews have made significant contributions to the cybersecurity field. The work investigated and analyzed the importance of artificial immune systems in IoT environments by evaluating and identifying the performance of empirical research on the approaches to secure IoT environments.

Smart City [3]

Smart City refers to the city that integrates modern day tech. Studies show that 60 percent of the world will be living in urban environments by 2030. This large population requires the innovation of advanced technologies to make smart cities. Such systems require huge communication and the security threats associated with them have not been considered. Due to intensive communication, high complexity and high severity, attack surface and cryptography related issues have remained unresolved. This paper provides problems and solutions of smart city related cyber attacks and also presents factors affecting the same.

Most countries do not develop smart cities due to willingness to change, resource limitations and financial status. There are five components to smart cities, buildings, utilities, infrastructure, transportation, traffic management and the city itself. In technical terms, smart cities are the collaboration between government and private sector to deploy mobile cloud computing, Artificial Intelligence, Biometric technologies and other intelligent decision making. Smart cities aim to solve global problems such as climate change, limited resources, urbanization and high population growth. Smart cities aim to increase economic competitiveness and make the general population's lifestyle classier. The concept of becoming smart is as different as cities itself. There are 6 different dimensions of making cities smarter: smarter governance, smarter economy, smart people, smart mobility, smart living and smart environment. Smart cities are not just about deploying smart technologies but propagating the communication and interaction of high level electronic objects. RFID (Radio Frequency Identification System) and smart handheld devices make the ecosystem as well. Smart cities are complex and hugely interdependent systems which have political, economic, social and technical problems and solutions.

To measure how smart a city is, we look at the level of automation and computer systems it uses, in addition to the integration between its systems. The high integration leads to high operational interdependencies between the most critical systems to the simplest ones causing huge cascade attacks that damage the whole infrastructure. Furthermore, smart cities face issues in vulnerability testing, response and recovering plans. Finally, taking care of security is costly and getting enough budget requires a long process in the public sector.

The importance of securing cyber threats is greater for technologies like smart cities. Smart cities have multiple layers and high complexity of communication and interaction between them, leading to difficulties in securing the communication. Main issues in infrastructure are Cameras, communication networks, building management systems and transportation management systems. Some of the main issues of smart cities' infrastructure is eavesdropping, denial of service and theft.

Smart cities compute and process huge quantities of real time data and work with data driven technologies. Smart cities produce fine-scaled and exclusive data. The data that smart cities produce are called Big Data. Other systems convert small data into infrastructure datasets. There are systems that make locked data for the public called open data. There are five privacy related issues: One has to secure identity data which means identity of the personnel, spatial data which means protecting a person's location, financial data which means protecting a personnel's theft of card details, communication data which includes prevention of eavesdropping on people's conversations and location data which means prevention of theft of a person's location.

Most softwares for smart cities are deployed by their vendors without sufficient testing for cyber security. Such insecure software may lead to filling the system with fake data which causes systems to shut down and service termination. It is clear that different technologies have different gaps in solving their cyber security related issues and have low overlap in the solutions. The gaps are either due to the lack of technical research on the topic, lack of efficient methodology used as in the case of Connected and Automated Vehicles or due to inefficient practices that can easily be worked on such as in the case of Smart cities.

Studies estimate that 60 percent of the globe will be living in urban surroundings by 2030. Smart cities must be created in order to accommodate this big population. Such systems necessitate extensive communication, and the security risks

[3] AlDairi, Anwaar, and Lo'ai Tawalbeh. "Cyber Security Attacks on Smart Cities and Associated Mobile Technologies." Procedia Computer Science, vol. 109, 2017, pp. 1086–1091, 10.1016/j.procs.2017.05.391.

they provide have not been taken into account. Attack surface and cryptography-related challenges have remained unaddressed due to intensive communication, high complexity, and high severity. Fog computing, smart cities, and Industry 4.0 have all seen substantial growth in recent years thanks to the Internet of Things (IoT), which executes the complicated data processing of sensitive information that must be safeguarded against cybersecurity assaults. As early as 2025, CAVs are anticipated to be in use for business purposes. Contrarily, CAV cyber security concerns have not received the same attention as other CAV technologies, despite their crucial importance and high priority in the most recent CAV advances. Cyber-attacks in CAVs may have major repercussions, including the loss of personal information as well as physical harm or even death.

2. Conclusion

Most technologies used today are either lacking in technical differences when it comes to efficient and secure systems. Some of the issues highlighted are that the vendors in the example of smart cities deploy the software without sufficient testing. Such insecure software may result in the system being overloaded with bogus data, which would cause systems to crash and services to be terminated. Each technology stated above has distinct literature and zero to none overlap in the methods used such as gradient boost in CAVs. One of the ways to develop smarter or efficiency would be to try to find how one methodologies from system 1 could be used in system 2 or vice versa. In the case of CAVs, the majority of research has been concentrated on a few distinct assaults, such as adversarial attacks that are particular to algorithms or location spoofing. Due to the fact that most research solely focuses on theoretical issues, there are not enough datasets and, consequently, not enough detection techniques. It is notable that both machine learning algorithms fared poorly on attack types, specifically mailbomb, udpstorm, httptunnel, worm, and xsnoop, which were only included in the testing data set. All five of these assault types had an accuracy of zero, which indicates that none of them were recognised. This is because Decision Tree and Naive Bayes both develop their models through the use of supervised learning, which makes it impossible for them to recognise previously unidentified attack types. Building classification or grouping models for previously unknown sorts of attacks is still an exciting area for future research.

3. Future Directions

Future Research should be conducted on upcoming technology related cyber security issues such as those in Brain-Machine Interfaces, Satellites, Cloud Of Things, and should focus on using higher end computing methods such as exascale, optical or neural computing to solve cyber security related issues that are not secure by current methods such as Quantum technologies. As discussed previously, cybersecurity is an immense threat to companies, individuals and governments alike and need to be tackled before malicious hackers can create the code that could cause disruptions at large levels. What could be the possible downcomings of current research and methodologies on machine learning based detection methods is a question that is very important for future research.

References

[1] AlDairi, Anwaar, and Lo'ai Tawalbeh. "Cyber Security Attacks on Smart Cities and Associated Mobile Technologies. " Procedia Computer Science, vol.109, 2017, pp.1086–1091, 10.1016/j. procs.2017.05.391.

[2] M. Handte, S. Foell, S. Wagner, G. Kortuem and P. J. Marrón, "An Internet-of-Things Enabled Connected Navigation System for Urban Bus Riders, " in IEEE Internet of Things Journal, vol.3, no.5, pp.735-744, Oct.2016, doi: 10.1109/JIOT.2016.2554146.

[3] S. Sangkhapan, P. Wannapiroon and P. Nilsook, "Development of Smart Bus Management System Using NB-IoT, " 2021 3rd International Conference on Computer Communication and the Internet (ICCCI), Nagoya, Japan, 2021, pp.152-156, doi: 10.1109/ICCCI51764.2021.9486773.

[4] Chauhan, H., Gupta, D., Gupta, S., Kumar, D. (2021). IOT-Based Electronic Ticket Device for Environmental Conservation Using GSM Module. In: Goyal, D., Gupta, A. K., Piuri, V., Ganzha, M., Paprzycki, M. (eds) Proceedings of the Second International Conference on Information Management and Machine Intelligence. Lecture Notes in Networks and Systems, vol 166. Springer, Singapore.

[5] Jessica Castro, Iury Araujo, Eudisley Anjos, and Fernando Matos.2017. A Survey on Bus Monitoring Systems. In the International Conference on Computational Science and Its Applications. Springer, 220-- 23

[6] T. M. Bojan, U. R. Kumar, and V. M. Bojan.2014. An internet of things based intelligent transportation system. In 2014 IEEE International Conference on Vehicular Electronics and Safety.174-- 179

[7] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash.2015. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Communications Surveys Tutorials 17, 4 (Fourthquarter 2015), 2347-- 2376.

[8] Tianqi Chen and Carlos Guestrin.2016. Xgboost: A scalable tree boosting system. In Proceedings of the 22nd acm sigkdd international conference on knowledge discovery and data mining. ACM, 785-- 794

[9] G. Choudhary and A. K. Jain.2016. Internet of Things: A survey on architecture, technologies, protocols and challenges. In 2016 International Conference on Recent Advances and Innovations in Engineering (ICRAIE).1-- 8.

[10] Emanuel F. Coutinho, Maurício M. Neto, Leonardo O. Moreira, and José Neuman de Souza.2018. Analysis of Elasticity Impact in Hybrid Computational Clouds. In Proceedings of the Euro American Conference on Telematics and Information Systems (EATIS '18). Association for Computing Machinery, New York, NY, USA, Article Article 25, 8 pages.

[11] Emanuel F. Coutinho, Paulo A. L. Rego, Danielo G. Gomes, and José Neuman de Souza.2016. An Architecture for Providing Elasticity Based on

Autonomic Computing Concepts. In Proceedings of the 31st Annual ACM Symposium on Applied Computing (SAC '16). ACM, New York, NY, USA, 412-- 419.

[12] Pedro Cruz Caminha, Rodrigo de Souza Couto, Luís Maciel Kosmalski Costa, Anne Fladenmuller, and Marcelo Dias de Amorim.2018. On the Coverage of Bus-Based Mobile Sensing. Sensors 18, 6 (2018), 1976.

[13] Samy El-Tawab, Raymond Oram, Michael Garcia, Chris Johns, and B Brian Park.2017. Data analysis of transit systems using low-cost IoT technology. In 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops). IEEE, 497-- 502.

[14] Xiaojian Feng, Jiuling Zhang, Jinhong Chen, Guoqing Wang, Liuye Zhang, and Runze Li.2018. Design of Intelligent Bus Positioning Based on Internet of Things for Smart Campus. IEEE Access 6 (2018), 60005-- 60015

[15] Sakari Jäppinen, Tuuli Toivonen, and Maria Salonen.2013. Modelling the potential effect of shared bicycles on public transport travel times in Greater Helsinki: An open data approach. Applied Geography 43 (2013), 13-- 24.

[16] R. C. Jisha, A. Jyothindranath, and L. S. Kumary.2017. Iot based school bus tracking and arrival time prediction. In 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI).509-- 514.

[17] Guerra, E. Planning for cars that drive themselves: Metropolitan Planning Organizations, regional transportation plans, and autonomous vehicles. J. Plan. Educ. Res.2**016**, 36, 210–224.

[18] Autonomous Vehicles|Self-Driving Vehicles Enacted Legislation; NCSL: Washington, DC, USA, 2019.

[19] Madrigal, A. C. Inside Waymo's Secret World for Training Self-Driving Cars. The Atlantic, 23 August 2017.

[20] Dikmen, M.; Burns, C. M. Autonomous driving in the real world: Experiences with tesla autopilot and summon. In Proceedings of the 8th International Conference on Automotive User Interfaces and Interactive Vehicular Applications; ACM: New York, NY, USA, 2016; pp.225–228.

[21] Eustice, R. University of Michigan's Work Toward Autonomous Cars; Technical Report; University of Michigan: Ann Arbor, MI, USA, 2015.

[22] Fagnant, D. J.; Kockelman, K. Preparing a nation for autonomous vehicles: Opportunities, barriers and policy recommendations. Transp. Res. Part A Policy Pract.2**015**, 77, 167–181.

[23] Ring, T. Connected cars–the next target for hackers. Netw. Secur.2**015**, 2015, 11–16.

[24] Dolev, S.; Krzywiecki, L.; Panwar, N.; Segal, M. Certificating vehicle public key with vehicle attributes a (periodical) licensing routine, against man-in-the-middle attacks and beyond. In Proceedings of the SAFECOMP 2013-Workshop ASCoMS (Architecting Safety in Collaborative Mobile Systems) of the 32nd International Conference on Computer Safety, Reliability and Security, Toulouse, France, 27 September 2013

[25] Amor, N. B.; Benferhat, S.; Elouedi, Z. Naive bayes vs decision trees in intrusion detection systems. In Proceedings of the 2004 ACM Symposium on Applied Computing; ACM: New York, NY, USA, 2004; pp.420–424.