International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 07 | July 2020 www.irjet.net p-ISSN: 2395-0072

Cyber Attacks on Smart Cities and How Artificial Intelligence can be Used as a Boon

Rohit Nandan[1], S. Rakesh Kumar[2]

[1]*Student, School of Computing Science and Engineering, Galgotias University Greater Noida, India*
[2]*Assistant Professor, School of Computing Science and Engineering, Galgotias University Greater Noida, India*

Abstract— *Smart cities are the future of human civilization. The World is approaching towards AI orientation where every other domain will have the involvement of Artificial intelligence. It is not too far, when most of the human work is going to be replaced by AI. IT Giants like Tesla, Google are working on AI since very long to help them making the cities smart. Another aspect which ensue with the evolution of AI is the security domain which is a major concern. The imagination of majority of AI driven Instruments in the wrong hand pose a catastrophic danger. In future, smart cities will largely depend on technologies namely Cloud, IoT, VANET, MANET.*

These technologies are existing in this world for a long span of time uncovering all the possible vulnerabilities and breaches to the white as well as dark world. Responsible Disclosure of these vulnerabilities are done only by human which might steer to some of the vulnerabilities being undiscovered.

This paper will unearth the methodologies to discover most of the known vulnerabilities with zero-day vulnerability and threats using Artificial Intelligence. This paper will also enlighten most of the possible threats to a smart city. A model is proposed in the paper for a general approach of securing the world from new and upcoming threats in the future.

Keywords—*Artificial Intelligence, Cyber attacks, IoT, VANET, MANET, Cloud, Vulnerability, threat.*

I. INTRODUCTION

As for the definition, Smart city is the community of urban people where different categories of IoT devices, sensors, and devices are used to collect different types of data from these devices to get insight of all these data eventually benefit the humankind. All these resources are managed by these sensors, giving more explicit and valuable information for automatic traffic light control system, water management system etc. Countries are stepping it up a notch to make their city's framework smart. Most of these smart city's framework including the resources, governance, people, education, health are managed through information and Communication Technology (ICT). A smart city means smarter growth.

A. IoT

Internet of Things (IoT) is the major yet emerging technology used in smart cities. As a saying, with great technology comes the greater threats, most part of the smart cities will work on IoT technologies which will make it prone to the attacks. IoT devices also gave contribution in Human-machine interaction. One of the important technologies used is RFID (Radio Frequency Identification System) which is susceptible Tag cloning attack. IoT devices are also prone to bot attack. Even though with the latest technologies, Plethora of IoT devices can become vulnerable by bot attack by the cyber attackers as well.

B. Biometrics

Biometrics is the automatic recognition of a person's trait based on some of the parameters namely facial traits, expressions etc. Biometrics plays an important role in system security. It equally secure many variable in the field of health, education, utility, patrol and security. Cyber attacks like Biometric spoofing and data breach are lethal to human resources.

C. Smart Grid

Most of the resource and infrastructure management in a smart city is done by Smart grid. All this is done by the communication instruments of sensors and IoT devices in real time. Failure to any of the management instrument leads to disconnection of various sensors and resources. Some of the major reason for failure are:-

- Threat to Data Integrity: False data injection from the sensors and devices may lead to theft of data integrity.
- Threat to Devices: Most of the IoT devices are prone to physical damage.
- Threat to Network availability: Most prominent attack to networks is Denial of Service (DOS).

As increment in the technologies bring increment in the Cyber threats, Smart cities can be of great benefit to the

mankind as well as a major catastrophe if misused. Cyber threat, a vulnerability that might be exploited to cause people or a community unknown and potential harm, are the most effective and threatening danger to smart cities which can cause severe harm to the people and resources. Many of the vulnerabilities have very high severity according to Common Vulnerability and Exposure (CVE). As Ethical hackers and researchers constantly finding the potential vulnerabilities and loop holes In the technologies used in smart cities or going to be there in future, Black Hat hackers and cyber attackers are continuously trying to breach the security. After all, there are humans who are finding bugs and vulnerabilities in the technologies like Cloud, IoT, VANET, MANET which in future are going to sustain a major part in the smart cities. Ethical hackers may find 99% of the vulnerabilities but may not be able to find every trivial bug which can be of great importance as far as hacker's perspective. Those 1% threats which might get avoided by the researchers can be of utmost importance as attacker point of view to exploit and use it against the people, their resources and might shutdown all the system in the smart cities.

Artificial intelligence, here can be of great use here as AI can work more efficiently and can produce more bugs and vulnerabilities than a human mind can discover. Based on all the historical data, training of the system will produce all the possible bugs and vulnerabilities of the technologies based on the historical data. Machine learning, can be applied here as Predictive analytics with the concept of AI will be useful to achieve the desired goal.

Technologies on one side helps human civilization to evolve but on the other posses greater threats if compromised. Increment in cyber attacks is mainly the repercussion of new technologies. Every day is the witness of new technology which no same as the older one. Now nearly every resource is available to the dark world, to exploit even the latest technologies which exist with the greatest security. The attackers nowadays also have the knowledge to how to dodge even the most secure machine well equipped with the firewalls and anti-viruses. For instance, anti- viruses and firewall maintain a database of different attacking signatures to prevent the cyber attack such as a .dll or any other file with different extensions, but attacks are performing vector attacks which might be attached with any document or PowerPoint which a firewall or anti-virus can't detect.

Many security proving companies are now enabling sandbox security in their Client's environment to protect them from a potential cyber attack. A sandbox technique is more or less like a honeypot where a virtual environment is provided at the end- user to test any type of malicious code. It also prevents majorly from a ransomware attack where only the pseudo files present in the virtual environment are encrypted and the original files on the machine are safe. Regardless of proving all the majors to prevent the security attacks, Zero-day Vulnerability is still a headache as security point of view.

It is true that Artificial Intelligence has helped different machines equipped with latest technologies to be secured but as mentioned earlier these methods are also not hidden from the attackers. Now many resources such as anonymous servers, VPN, Onion Routing browsers for anonymity such as TOR are available for the attackers as well. Using AI, before attacking any particular machine, they analyze using AI on the upper hand, whether they are attacking a virtual environment or the original machine. So, to tackle such attacks, Artificial Intelligence Can be used as a mitigation for such attacks. By Using Predictive Analytics, Artificial Intelligence can be a major panacea for these emerging cyber attacks against emerging technologies in the different aspects of IT industry.

As under the predictive analytics, based on the transitional data and previous attacks, prediction of attacks in the future will be encountered before happening. Predictive analytics by measuring different relationship among different factors to analyze and provide weightage to different aspects. Predictive Analytics using Artificial Intelligence is going to increase the accuracy for the Prediction. This Paper would likely propose a model to implement the Predictive Analytics on the coming cyber attacks.

II. PRESENT SCENARIO

Today Renounced IT Giants like Tesla, Google, Microsoft are working with their heart and soul to apply Artificial Intelligence algorithms and equations in future deploying technologies namely cloud, VANET, smartphone technologies, RFID, biometrics etc but have not found any achievement so far. But ethical hackers and researchers are the only prime source to discover vulnerabilities and bugs in IoT devices, algorithms, websites and web applications. This might lead to revealing most of the threats but most of them are either been discovered by attackers already or the solution is already existing using which many attackers are able to perform highly aggressive attacks on the resources of smart cities causing them high mutilation of both resources and people.

There are possibly infinite number of possible cyber threats to the resources, websites, web applications that you can think of. A table is mentioned below to analyze maximum cyber threats to a smart city, their resources which can jeopardize the security of the resources.

TABLE I: Various types of threats to smart city

Cyber Threats	Security	Affecting Areas	Description
Denial Of service	Medium	WEB services, weather sirens	Legitimate requests are denied due to high traffic generated by false requests, botnet.
Man in The Middle Attack	Medium, high	Traffic lights, train control system	The attacker acts as the mediator between sender and receiver.
Side Channel Attack	Medium	Communication networks	Attacks by extracting the integrated information from physical parameters rather than executing direct attack. Useful in communication attack.
Spoofing	Medium	Surveillance cameras	Acting as a disguise by responding to the legitimate request. It helps in gaining access to security cameras.
Botnets	Medium	DOS, DDOS	Small malicious codes that act to the command by the attacker. Major help in DOS and DDOS.
Zero day attack	Medium, high	Every area of smart city can be affected	An attack which has not been discovered till date and does not contain any log or database. Prime concern to smart cities.
Tag cloning	Medium	Communication networking	Copy of genuine EPC tag to hazzle the radio frequency Identification (RFID). Hampers the communication signals.
sniffing	Medium	Power grid, IoT devices	Capturing and analysing data packets using potential packet analyser to jeopardize the security.
Distributed Denial of service (DDOS)	High	Water supplies, power grid	Similar to DOS but uses bots stored on different systems to attack a service.
trojan	High	Automated vehicle system, traffic lights	Malicious code which is attached with a potential software and executed in the background under the control of the attacker.
Payload in the functional code	High	Vehicle system, communication system, IoT	Small malicious code written in the functional code for smart cities technologies that lead to improper functionality of the program or application.
Session hijacking	Medium, high	IoT devices, automated vehicles	Any connection which seems genuine but was conducted by the attacker himself. Great risks to the automated systems.
Social Engineering	Medium, high	Every possible Technology	Reconnaissance done in order to gain security information by social means.
SQL injection	High	Data breach, cloud	Injecting SQL queries to retrieve sensitive data from the databases.
Poor encryption	Medium, high	Data stealing, data breach	Encrypted data transfer may be revealed if poor or obsolete encryption technique is used

III. PROPOSED SOLUTION

The model which will have analytical approach will work in five phases to be implemented over any machine or to prepare for a cyber attack. This model will contain different levels of implementations.

A. Signature Dictionary

Different cyber attacks such as botnet attack on IoT devices or Ransomware attack on a particular host , all have different signatures by which these attacks are identified. The malicious programs might contain some specific keywords arranged in specific manner which might identify them as malicious program. Different techniques are used by the attacker to bypass the firewall such as malicious code will not appear malicious

to the firewall or anti viruses as the signature are being changed but works in the same malicious way.

So, a dictionary which contains all the previous data which has malicious keywords along with the similar code which can be used to bypass the security is made in the first phase of this model. The dictionary is able to detect keywords which can be used maliciously such as @echo, [/script], alert(0), SQL injections such as ";1=1 also with all the possible nearest

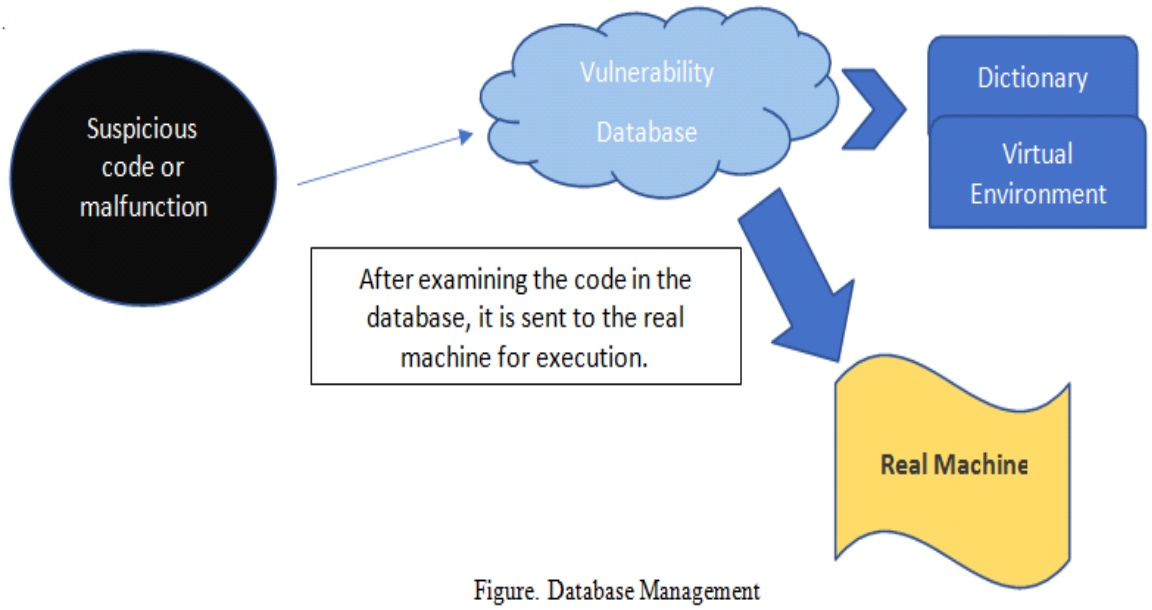

Figure. Database Management

keywords which might come under the category of malicious code. Such programs are kept and send with the report to the authority for examination.

B. Database

Security companies maintain the record of every attack and known malicious codes with them. They maintain a database which contain all the information about the threat such as the origin, creator, first time use, attacker info, threat ID, Severity rate etc which helps them categorize the new and coming threats. As there is information present in CVE(Common Vulnerability and Exposures) about every threat and cyber attack known, under this model a vulnerability database is maintained where all the required resources for the model are present such as the signature dictionaries, Pseudo data for testing, virtual labs etc. Whenever any attack happens, the information will be send to the database, it will match the signature with the signature present in the dictionaries. Afterwards, the code or program will be run in the virtual environment on the virtual data to detect any unusual behaviour. If the program performs unusual behaviour, the code will not be executed on the real machine and the signature will be added to the signature dictionary

C. Behavioral Analysis

A cyber attack might not in the beginning seem as an attack, as the attacker plans and do reconnaissance for a long span of time before placing an attack. Unless sometimes, the whole attack is executed successfully then the victim came to know. So in the third phase of the model which is most important phase of the model, the machine is properly analysed and observed for even a slightest change in the environment of the machine. The machine if encountered any change will report the change which might be a cyber attack. This feature of the model will encounter the attack even before happening. This will reduce the chance for a potential cyber attack which have a devastating affect on the resources of smart cities. Further phases will highlight more on the technical and statistical approach of the model.

D. Statistical Approach

Different security techniques are used today for securing both real time and run time environment. Such techniques based on different algorithms which helps in implementing the technique on the data as well. To predict a cyber attack many technique such as sandboxing are used by security experts to prevent it. According to data, we can predict the attacks based on different aspects such as solution to security technique, dictionary maintenance. The model is helpful for securing the machines based on previous attacks.

E. Accuracy

By all the data collected in the vulnerability database of this model, the accuracy will also escalate. This model initially maintain the dictionary with all the known data and new data will automatically be stored on the servers which helps in gaining the accuracy. Moreover, This model will gather information from different database which increase it accuracy significantly. The power of this model is its increasing accuracy by the time.

F. Future Scope

This model is accurate for securing almost any technology or technology coming in future. Future cyber attacks are going to be more sophisticated than in present but this model in general will sustain then also. Some amendments in the future can be done in this model to add more points. This model can work with different frameworks of security providing reliable secure environment. This approach in the future might help in the development of other models which will contribute in the security from the attacks in future. Many new ways for the cyber attacker will also emerge ahead.

IV. Conclusions and Recommendations

Based on different phases proposed in the above model, it can be concluded that primarily Cyber attacks are the part of Technical world which we cannot deny but it can surely be encountered using different security measures. It can be stopped before happening using above model. This model is basically recommended to be used along with different algorithms to escalate the security of the machines as well as the technology. In future, the smart cities which will surely adopt many new and emerging technologies can use the model based on the analytical approach to secure the resources of the smart city and the people. In future, this model can also be simplified and added with new approaches to enhance the upcoming technologies and resources.

REFERENCES

- A.Alibasic, R.Al Junaibi, Z.Aung, W.Lee Woon, and M.A. Omar," Cybersecurity for Smart Cities: A Brief Review," Lecture Notes in Computer Science January 2017
- S.Ijaz, M.Ali Shah, A. Khan and M.Ahmed,"Smart Cities: A Survey on Security Concerns," (IJACSA) International Journal of Advanced Computer Science and Applications,Vol. 7, No. 2, 2016, pp. 612- 625
- N. Kolla, M. Giridhar Kumar," Supervised Learning Algorithms of Machine Learning: Prediction of Brand Loyalty" International Journal of Innovative Technology and Exploring Engineering (IJITEE)ISSN: 2278- 3075, Volume-8 Issue-11, September 2019, pp. 3886-3889
- R. Devakunchari, Sourabh, P.Malik," A Study of Cyber Security using Machine Learning Techniques," International Journal of Innovative Technology and Exploring Engineering (IJITEE)ISSN: 2278-3075,Volume-8, Issue-7C2, May 2019,pp. 183-186
- Z.Allam, Z.A.Dhunny," On big data, artificial intelligence and smart cities," 17 January 2019, https://doi.org/10.1016/j.cities.2019.01.032,pp. 80-91
- A.S. Elmaghraby, M.M.Losavio," Cyber security challenges in Smart Cities:Safety, security and privacy," 5 March 2014,pp. 492-497
- A.AlDairi and Lo'ai Tawalbeh," Cyber Security Attacks on Smart Cities and Associated MobileTechnologies," The International Workshop on Smart Cities Systems Engineering (SCE 2017),pp. 1086-1091
- X.D.Hoang and N.T.Nguyen." DetectingWebsite Defacements Based on Machine Learning Techniques and Attack Signatures," 8 May 2019
- A.I.Vodă and Laura-Diana Radu," Artificial Intelligence and the Future of Smart Cities," Broad Research in Artificial Intelligence and Neuroscience, Volume 9, Issue 2 (May, 2018), ISSN 2067-8957,pp. 110-127
- Osisanwo F.Y, Akinsola J.E.T, Awodele O, Hinmikaiye J.O, Olakanmi O. and Akinjobi J.," Supervised Machine Learning Algorithms: Classification and Comparison," International Journal of Computer Trends and Technology (IJCTT) – Volume 48 Number 3 June 2017,pp. 128-138

- K.E.Skouby, P.Lynggaard, I.Windekilde and A.Henten," How IoT, AAI can contribute to smart home and smart cities services: The role of innovation," 25th European Regional Conference of the International Telecommunications Society(ITS), Brussels, Belgium, 22-25 June 2014
- D.Inclezan and L.I. Pr_adanos," Viewpoint: A Critical View on Smart Cities and AI," Journal of Arti_cial Intelligence Research 60 (2017),pp. 681- 686
- B.Chernis and Dr. R.Verma," Machine Learning Methods for Software Vulnerability Detection," IWSPA'18, March 21, 2018, Tempe, AZ, USA,pp. 31-39
- RL. Russell, L.Kim, L.H. Hamilton, Tomo Lazovich, Jacob A. Harer, O.Ozdemir, P.M. Ellingwood, M.W. McConley," Automated Vulnerability Detection in Source Code Using Deep Representation Learning," 17th IEEE International Conference on Machine Learning and Applications (IEEE ICMLA 2018)
- L.Zhao,Z.Chen,Q.Jia,"Summary of Vulnerability related technologies based on Machine learning," Advances in Materials, Machinery, Electronics II AIP Conf. Proc. 1955, 040054-1–040054-4; https://doi.org/10.1063/1.5033718
- Nanni G. (2013/. Transformational 'smart cities': cyber security and resilience. Symantec, Mountain View, CA.
- Elmaghraby AS, Losavio MM. Cyber security challenges in Smart Cities: Safety, security and privacy. Journal of advanced research. 2014 Jul 31;5(4):491-497.
- National vulnerability database. https://nvd.nist.gov. Accessed: 2017-07- 01.