International Journal of Research in Circuits, Devices and Systems

E-ISSN: 2708-454X
P-ISSN: 2708-4531
IJRCDS 2021; 2(2): 49-54

www.circuitsjournal.com
Received: 07-05-2021
Accepted: 10-06-2021

Ronodeep Das
School of Computing Science and Engineering, Vellore Institute of Technology, Chennai, Tamil Nadu, India

Correspondence
Ronodeep Das
School of Computing Science and Engineering, Vellore Institute of Technology, Chennai, Tamil Nadu, India

Survey of honeypot-based threat detection systems

Ronodeep Das

Abstract
In a growing world of networking and data, prioritising network security is extremely important. Various methodologies for protection of networks and its data have been developed over the years and continue to be developed. However due to the increase in the sheer amount of people using networks throughout the world network security itself is becoming a harder task. Since there is already a multitude way of attacking networks and more developing everyday it is extremely difficult to keep track of them while the users of the network participate in it. Honeypot-based network security systems help in solving exactly this problem. It is essentially a system designed to recognise threats to a network by baiting and trapping those threats into a system that isn't actually being used by the people, making is easier to detect and keep track of threats. Furthermore, since Honeypots are essentially running fake systems for detection of intrusions, they also consume less resources while providing an environment to gather extensive data on intrusions, hacking processes and techniques and other attacks. This paper presents a survey of the techniques and advances that Honeypot based systems have brought into Network Security. This paper also provides a review of the various types of Honeypot systems that are being used in network security and how Honeypots are being applied in the industry. Next, the article gives a brief overview of more advanced Honeypot-based technologies that are in development and will be paramount in the advancement of network security in the future. Finally, several open issues and research trends are outlined.

Keywords: Network security, honeypots, cyber-attacks, botnet, ethical hackers

1. Introduction
With the increase in the use of computing technologies such as phones, laptops, PCs etc. the number of devices connected to networks and use of networking itself continues to grow at a tremendous rate. Especially after the onset of the COVID-19, which forced much of the world into isolation, the only way of communication that wasn't dangerous was the digital way, so even people who were previously not massively in dependence of modern technology, had to give in so as to keep up their work and communication. This lead to an increase in the data and information that is being transferred over networks from one point to another, much of it sensitive and important. But this uptick in data transfer through networks has also resulted in the attackers/intruders/hackers and the like to increase their attacks, probing and other malicious actions to get access to such data. Since security also keeps increasing, newer and more advanced, innovative methods are created by people to crack the securities and gain access to the data, and while the amount of people trying to do so are untraceable, they keep increasing, in numbers and in the ways in which the execute their malicious actions, making it difficult for traditional security methods to keep up. An anti-virus, firewall or Intrusion Detection System are all important for security, but they are limited to the methods which they are built to counter for the most part, making it difficult to adjust them for latest attacking methodologies and techs. This is where Honeypot technologies can help in increasing network security of systems against the constantly evolving sea of attackers.
Honeypots are essentially a technology which works on the basis of luring attackers to attack a system which isn't the real system itself, but instead a decoy filled with certain services and vulnerabilities that the attackers may find attractive and try to attack. This decoy system is monitored for attacks and the data regarding attacks, such as the methods used, the target of attacker, address and other information are acquired and stored. This data is analysed and through this data improvements to the original system are made improving the security of the system itself without compromising it, in most cases. Basically, a honeypot is "A program that takes the appearance of an attractive service, set of services, an entire operating system or even an entire network, but is in reality a tightly sealed compartment built to lure and

contain an attacker" [1]. Many organizations and business have understood the capabilities and importance of a Honeypot system and are already using them. But new ways of using the technology continue to be developed in various fields of network related communication and data transfer.
This paper provides a survey of the various types of Honeypots and how they are generally classified, and the most important classifications, including the significance of the classifications. Honeynets, a type of honeypot network, which is also extremely useful is also covered. Along with those various ways in which Honeypots are being used in innovative ways to increase security of certain well-known systems and provide better threat detection and prevention are also listed. Finally certain future research trends and possible developments for the field are discussed.

2. Classification of honeypots
Honeypots are classified in several ways depending on different categories, however each of these classifications are significant and have been done for a reason. Among the different types of Honeypots listed below, a single Honeypot could be belonged to multiple types too. The classifications are as follows.

2.1 Based on usage
2.1.1 Production honeypots
Production Honeypots are used for protecting an organization's network containing its servers. They emulate operating systems, to lure the attackers. It is used to collect data regarding attackers who're attacking the production servers or the internal networks of the business/organization. It may collect data such as originating Internet Protocol (IP) addresses, traffic frequency and volume, directories accessories and more. It is essentially a way of mitigating risks in an organization. It can launch fake services to analyze the attack on the servers of the organization. They are deployed alongside the actual production servers to run the same services or positioned internally within the server. It is preferred by businesses/organizations because it is easy to use and implement while at the same time revealing the threats and loopholes existing in the systems of the organization. The organization however still needs to have other security services such as firewalls, intrusion detection systems, and more to ensure complete protection because while the features provided are good, they still fall short of certain attacks and hence can still be breached by certain attackers.

2.1.2 Research honeypots
Research honeypots are used for collecting extensive data and analysis regarding the attacks on a server/network as compared to Production Honeypots. They aren't generally used by most businesses/organizations but are used by the government, universities, military or research organizations. Unlike production honeypots, which are deployed alongside or within a business's network, research honeypots are deployed in multiple networks or locations to gather more information about the actions of the intruders. They are also used for educational purposes. Research honeypots are more complex to implement and require more work for deployment as compared to production honeypots but at the same time provide much more information regarding the system's threats, attackers and vulnerabilities and loopholes can be gathered. Similar to production honeypots they contain non-genuine data and services that is made to look important to hackers/attackers to lure them into attacking the system and hence gaining information about them.

2.2 Based on level of interaction
2.2.1 Low interaction honeypots
Low Interaction honeypots, as the name suggests, provide very limited interaction and access to services and resources to the attackers of the system. Since it is meant to provide only limited access, low interaction honeypot does not contain or represent a complete system for the attacker to exploit rather only certain services such as ftp or http, or protocols like TCP and IP. They are simple to deploy and aren't very complex and hence the amount information that can be collected about the intruder through it is also limited. The amount of network services and protocols emulated by a low-interaction honeypot is dependent on its design, but the amount emulated is generally minimal and just enough so as to lure the attacker into believing that a real system is being attacked. The complexity of the security system is also reduced since low interaction honeypot consume less resources and less code. An example of a low interaction honeypot is Honey D.

2.2.2 High interaction honeypots
High interaction honeypot features a fully-fledged system for intruders/attackers to interact with, as in the services, protocols, systems aren't emulated but real. Since the system provided to be attacked is real, it does a good job of luring attackers who're generally more careful regarding attacking systems and are watching out for traps. Furthermore, since complete access is provided the amount of data and information that can be collected regarding the attackers is immense. When the attacker enters the honeypot system, his actions can be monitored in extreme detail, such as what techniques he uses to gain privileges, what privileges he makes use of, the directories and information that are accessed, the types of tools utilized by the attacker, how he hides his actions and more. This provides a good environment for researching certain attacks/attackers and gathering extensive data about them. Although the system is real and not emulated, it is still a decoy for luring attackers. Therefore, almost any traffic that is found in the system is possibly malicious and is probably the sign of an attacker since the system isn't meant to hold regular traffic of the network. However high interaction honeypots are difficult to implement and deploy but in return provided, as stated before, more information regarding the attackers. However, they also possess risks, since a high interaction honeypot features a complete system, it can also be compromised by an attacker, once compromised the attacker can start to attack other hosts on the internet or use the compromised machine for other malicious purposes. The main system also becomes more vulnerable once the decoy system falls. Therefore, it's important to mitigate these risks by keeping some additional defensive options available for the system, such as firewalls and Intrusion Detection Systems (IDS). Examples are Mantrap and Honeynets.

2.2.3 Medium interaction honeypots
Medium interaction honeypots lie in between high and low interaction honeypots. They are essentially made to combine the benefits of both high and low interaction honeypots.

They are less complex than high interaction honeypots but more complex to deploy than low interaction honeypots generally. Medium interaction honeypots don't have a full operating system environment to be interacted with, and don't have all the application services and protocols either. They work on the basis of virtualisation. They await attackers and give responses to the attackers that are just sufficient enough to lure them into getting more information about their attacks and techniques. Once the attacker sends his payload, the shell code of the payload is extracted and used as a source of information. If there is some malware in the payload then through the information gathered the malware is stored somewhere in the system or in another virtual system for further analysis in the future. However medium interaction honeypots are extremely hard to build, require immense effort and must have fine emulation for every response that is to be emulated and is extremely difficult to build when the system is not fully operational like high interaction honeypot or has simpler mechanisms like low interaction honeypots.

2.3 Based on hardware deployment type

2.3.1 Physical honeypot

Physical honeypots are type of honeypots that run on single real machine with a real operating system and services. They are nearly always high-interaction and hence allow the system to be compromised completely. This makes them cost intensive as they need to be installed and have been maintenance done. It has its own IP address as well. So, the responses and studies done on the honeypot are done on real systems.

2.3.2 Virtual honeypot

A virtual honeypot is a software that runs on a physical system to emulate a virtual environment of another system that is used to lure in attackers and is specifically meant to be probed in order to collect data regarding the attacker. It is designed to resemble the actual network much like the original honeypot definitions suggests, except on a virtual environment on a real machine rather than running the system that is luring the attackers on the real machine itself. Several of them can be hosted in single real (physical) machine. Example AGROS.

3. Honeypot security applications

There are various applications to Honeypot Security methods, some of the innovative ones are listed as follows.

3.1 Honeypot for LAN security

Honeypot System can be especially used for detection of threats and protection from them in a LAN environment depending on how the system is setup. "The traditional defense usually gives inadequate performance in face of the new invasion, so the honeypot can be deployed to the LAN to conduct active defense. The network security solutions proposed in this paper are based on the honeypot system. To deal with some suspicious network connections, the system will no longer block them, but introduce them into the honeypot system" [2]. Since LAN servers are more attractive to hackers, given the information and access they provide, the deployment of a honeypot system provides increased security for a LAN. A virtual honeypot server can be setup along with a physical honeypot. The virtual honeypot allows for cheaper but more secure system for the LAN. It can even discourage low level attacks/attackers from going through with the attack while also providing information regarding the same. A physical honeypot needs to be set in place in case a high-level attacker tries to intrude the system so that more information can be gained from the attack even if the virtual honeypot isn't able to accomplish as much as it can. Regardless of whether an attacker detects the system or not, if contact occurs the basic information regarding the attack can be discerned which can then be used to improve the defences of the LAN. An example of a low interaction honeypot that can be used for a LAN is Open Canary, an open source honeypot software written in python.

3.2 Honeypot security for mobile communication

Mobiles are extremely important commodity in the current world, with all the features that come with them, however since they possess so many features of storing data as well as the communicating data, protection of such data from malware and other attacks is also important. A Honeypot system can also be used for the observation and detection of threats in mobile communication systems. Much like other honeypot systems the core concept of the attacks being studied through the honeypot system acting as a lure for the attacks and hence information being gathered through it remain the same. However the reason why a honeypot based approach may be more effective than traditional ways is that the anti-virus/malware security systems for mobile are hardware based hence they have a low virus capture rate and utilise more resources. This combined with the fact that smartphones in today's generation are extremely diverse, hence security that are hardware based have inherent limitations to how much protection they can provide give more incentive to the application of Honeypot based mobile communication security system. As demonstrated in "A Mobile Communication Honeypot Observing System" [3] the efficiency of a mobile communication honeypot in GSM (Global System for Mobile Communications) is fairly reasonable. A honeypot system that is made with layered modules, and works in the following way: "In the system, mobile communication terminals (smart phones) can communicate in this "real" situation built by honeypot. At the same time, in the information interaction between mobile phones and mobile networks, the application processing center can track and observe a series of communication behaviors of mobile phones and test their safety. Protectors can use the observing result to find potential safety hazards and better the protective environment to achieve the goal of protection. "This is only a single proposed way of creating system for the security of mobile communication that overcomes the deficiencies that the current general systems possess, various other ways of applying the honeypot system for security can also be used.

3.3 Honeypot security for Bluetooth communication

Bluetooth Networks are typically used for exchange of data through radio-waves over short-distances in 2.402 GHz to 2.48 GHz frequency range and also for building PAN (Personal Area Networks). Bluetooths are also extremely commonly used by people, hence their security also becomes important. While a simple way of implementing Bluetooth security for an organization could be to restrict the Bluetooth communication to company owned devices, and also mitigate a possible attack on Bluetooth devices by ensuring that Bluetooth is enabled and disabled depending

on when it's necessary. Ensuring the safety of Bluetooth communication through rigorous methods is necessary to thwart high level attackers from attacking the Bluetooth network. There are various Bluetooth security methods available in market but Honeypots can also be used in this scenario as well for the detection along with study of attacks on a Bluetooth communication. An example of a Bluetooth honeypot is Bluepot developed my Andrew Michael Smith as a university project. It was designed to accept and store malware that was sent to it along with interacting with common Bluetooth attacks. The data can be monitored using a GUI that contains graphs, lists, dashboard along with log files. A study conducted on Bluepot [4] had various findings. It was concluded that while the system of was good at detecting the attacks, the information regarding the attacks was somewhat unreliable. The data that was logged such as attack time, address, protocols exploited and sensor logs was consistently produced. But unfortunately the data that was in logs was volatile as it would get deleted along with the termination of the program. However these short comings simply imply that the system can be improved upon and better and more advanced Bluetooth Honeypot systems can be made for better security in Bluetooth communication. As also concluded by the study that once these problems are worked on a tool like Bluepot could pose to be a very valuable tool for forensic examiners and security auditors.

3.4 Honeypot security for VoIP

Voice over Internet Protocol (VoIP) is a method for the delivery of voice communications and multimedia instances through Internet Protocol Networks. It essentially lets anyone place call over an internet connection. As internet and broadband access continues to grow so does the feature of VoIP. It's preferred over traditional analog phones because it's cheaper and provides more features. Hence again due to its popularity it's extremely important for its security to be on par, since it invites more attackers due to how popular it is, and more types of attacks. Due to the sheer amount go VoIP communication that is being held and will continue to be held, the attacks and the attackers also continue to find various ways to break through into those communications. While basic VoIP security and encryption are invaluable, a Honeypot system combined with the same will result in a system that is more prepared for the rising threats against VoIP communication. "VoIP Honeypot Architecture" [5] outlines the various threats that are posed to VoIP communications, most of which are generally known, such as Denial of Service attacks, Call Tracking, Call Hijacking, Password Cracking and user enumerating, SPAM over Internet telephony, Host based intrusions etc. but most importantly provides an approach regarding how to design a VoIP specific honeypot. The honeypot system outlined is a combination of various network tools which allow for monitoring of attacks on VoIP communication and gather information regarding them. It works on an enterprise domain where multiple user agents are served by an SIP proxy. Instead of using SIP protocol packets as traces of an attack, it gathers information in real time. The proposed system was named honey phone, but various changes to the proposed system probably need to be made in accordance with newer standards, however the template proposed for the application of Honeypot in VoIP remains the same. Newer and better templates can be made too.

3.5 Honeypot security for SQL injections

SQL injection is a web security vulnerability that gives access to the attacker to disrupt and/or impede with the queries that are being sent to the database of said web application. This involves giving the attacker access to data that they shouldn't have free access to such as data regarding other users, data regarding the application and its inner system etc. The attacker may use this data in varying malicious ways such as modifying the data, deleting it or redistributing the data illegally. In extreme cases the attacker may go as far as to comprise the whole web application's system. A honeypot security system can be applied in such a scenario for security against SQL injections as well, in-fact it proves to be extremely invaluable in the modern day. As while SQL injections are well known the functionality of various injections and how they work differ from one to another. This provides a perfect system for honeypots to be utilised in as they are built so that the vulnerabilities are exploited and the data from those exploitations/attacks can be used to improve the security of the system. This allows for the collection of data regarding the SQL injections. A type of honeypot that can be used to deal with SQL injections are High Interaction Honeypots (as discussed in a previous section). As described in "High-Interaction Honeypot System for SQL Injection Analysis" [6] which provides a profile of a High Interaction Honeypot which can be used for SQL Injection related threats. It is essentially a research type honeypot that is emulating a website with certain vulnerabilities. The honeypot system highlighted uses exception based and signature based detection techniques to develop a pattern matching engine for the complete analysis of the attack sequences later. This analysis can reveal the target, the degree of intrusion and methods used to obtain the target. After the attack, an attack graph is generated to provide large quantities of evidence to track regarding the attack and intruders. This is all done on a sandbox which is then used to recover the operation system after attack setting it back to its initial state for collecting data regarding any further attacks. This honeypot system is meant to lie between the web application and the database. There are various other honeypots that can be developed for dealing with SQL injections, including low interaction honeypots.

4. Honeynet

Honeynets are essentially simulated computer networks that contain vulnerabilities on a decoy server designed for testing the security of the network. It's essentially does what a Honeypot does just with an extremely high amount of interaction, and hence may be also called a subset of High-interaction Honeypots. The concept of Honeynets however is somewhat new as compared to the concept of Honeypots themselves. Unlike Honeypots which started development in 1990, Honeynets have been in development since 1999. It forms a group of virtual servers contained within a single physical server, in most cases and each of these servers are individual Honeypots. So it essentially forms a network of Honeypots, hence the name Honeynet. Each of these virtual systems possesses its own operating system and configurations depending on how the Honeynet is designed, however the crux of the concept is that it mimics the build of the system that is originally used in the business/organization. This gives the attackers full access to the operating system, the services etc. to interact with and

exploit.

The environment of a Honeynet isn't caged and the services aren't emulated, but this allows for a greater probability of the intruder being unable to detect that he has fallen into the trap. Furthermore since it is an entire network it allows for the intruder to completely navigate said network without posing a problem to the original network being protected and hence offers greater security than a single honeypot would on its own. Honeynets are also generally not meant for production (however they can be used as production honeypots depending on some cases), therefore any attacks that are being delivered to the Honeynet are most probably intruders that intend to probe, attack or perform other malicious actions to the systems, this decreases the likelihood of false positives and makes the process of dealing with information gathered regarding the attacks much easier.

As it is a network, not only will the services be vulnerable, as in general single honeypots, but the accessories which help in building the network, such as firewalls, routers, other network devices, will also be vulnerable. But the devices and services employed in the Honeynet do not contain any sensitive information that is available in the original network, so that even if the data is destroyed, compromised, modified, no damage to assets of the organisation occurs.

As addressed before Honeynets are generally not meant for production, and the reason has very little do with the capability of Honeynets, in-fact they can be quite beneficial to have as production Honeypots. But the resources, time required to build, design and implement a Honeynet is extensive. This makes them a poor choice for production Honeypots as opposed to other general production Honeypots which accomplish the same things with lower amount of assets and resources consumed.

The Honeynet project is a non-profit security research organisation that is working on the basis of this concept to develop security tools to improve internet security. They investigate latest attacks and based on the analysis obtained from Honeynet systems provide methods to increase the security of the systems involved. In 2002, the Honeynet they developed managed to capture a new tool that wasn't known before.

5. Further research

Since Honeypots it still relatively unsaturated in terms of the amount of research being done on it, there are various possible research opportunities in the field of Honeypot Security.

A promising prospect is the combination of Intrusion Detection Systems and Honeypots, while already having been in the field, the amount of research done on the topic and the material available is very low. This combination yields an even more powerful and dependable security system for any application or enterprise. "Sophisticated Honeypot mechanism-the autonomous hybrid solution for enhancing computer system security" [7] proposes an architecture that uses a sophisticated hybrid Honeypot with an autonomous feature as an IDS detection mechanism. This minimizes detection failures and improvement in the collection of important data. It also provides various points upon which further research and development can be done to create better systems that have lesser false positives while providing appropriate information.

Data mining is a well-known field with a variety of applications. It's application can also be used in Honeypot technology. Since the gathered data from various attacks and its analysis are an important of how Honeypot technologies provide value to a security system, data mining can hence also provide value to this aspect of Honeypot technologies to improve the how the data is dealt with so that more value can be obtained from it. As highlighted in [8] several projects have proposed data analysis tools and techniques for honeypots for taking benefit from data mining techniques such as artificial neural networks, genetic algorithm etc. More algorithms can be used and integrated that haven't been proposed yet from data mining techniques for the improvement of Honeypot technologies.

Peer to Peer (P2P) networking has been in the market for quite a while and has more recently seen popular use in certain areas. Software programs such as Bit Torrent, Morpheus etc. make use of P2P networking for transferring and exchanging data between the peers. While these networks are inherently less secure due to the very nature they are designed with, Honeypots can still provide some value and insight into how the security regarding such systems can be improved. For example in [9], the proposed concept uses the idea of a Honeypot and designs a method to trace who spread illegal and harmful contents in P2P networks and followed by storing this forensic evidence.

There are many other fields and aspects of networking and communication that be improved with the help of Honeypot technology with proper research regarding the same. The few highlighted above are a small sample. Further, researchers are suggested to refer articles [10-16] to know about cyber-attacks on critical systems, and several prevention systems for the same.

6. Conclusion

In this paper, the importance and need of more Honeypot technologies and their implementation is discussed. Followed by a discussion regarding the various types of Honeypots available in the market, the value the different type brings and their significance, which is important for understanding how each is used in various ways and contexts. Followed by classification, various innovative applications of Honeypot technology were discussed, how in various ways the concept of Honeypot is used to improve security in different forms of networking. Finally, we went over some research opportunities which can be researched upon in the future for further development of the field.

7. References

1. Joshi RC, Sardana A. Honeypots: A New Paradigm to Information Security. Enfield: Science Publishers, 2011.
2. Li Li, Hua Sun, Zhenyu Zhang. The research and design of honeypot system applied in the LAN security", IEEE 2nd International Conference on Software Engineering and Service Science, 2011, 360-363.
3. Song Y, Zhu X, Hong Y, Zhang H, Tan H. "A Mobile Communication Honeypot Observing System", Fourth International Conference on Multimedia Information Networking and Security, 2012, 861-865.
4. Podhradsky AL, Casey C, Ceretti P. The Bluetooth honeypot project, Wireless Telecommunications Symposium, 2012, 1-10.
5. Nassar M, State R, Festor O. VoIP Honeypot Architecture, 10th IFIP/IEEE International Symposium

on Integrated Network Management, 2007, 109-118.
6. Ma J, Chai K, Xiao Y, Lan T, Huang W. High-Interaction Honeypot System for SQL Injection Analysis, International Conference of Information Technology, Computer Engineering and Management Sciences, 2011, 274-277.
7. Vokorokos L, Fanfara P, Radušovský J, Poór P. Sophisticated Honeypot mechanism-the autonomous hybrid solution for enhancing computer system security, IEEE 11th International Symposium on Applied Machine Intelligence and Informatics (SAMI), 2013, 41-46.
8. Ghourabi A, Abbes T, Bouhoula A. "Data analyzer based on data mining for Honeypot Router", ACS/IEEE International Conference on Computer Systems and Applications-AICCSA, 2010, 1-6.
9. Lee H, Nam T. P2P Honeypot to Prevent Illegal or Harmful Contents from Spreading in P2P network, The 9th International Conference on Advanced Communication Technology, 2007, 497-501.
10. Meghna Manoj Nair, Amit Kumar Tyagi, Richa Goyal. Medical Cyber Physical Systems and Its Issues, Procedia Computer Science. 2019;165:647-655. ISSN 1877-0509, https://doi.org/10.1016/j.procs.2020.01.059.
11. Amit Kumar Tyagi, Aghila G. A Wide Scale Survey on Botnet, International Journal of Computer Applications (ISSN: 0975-8887). 2011 Nov;34(9):9-22.
12. Amit Kumar Tyagi. Article: Cyber Physical Systems (CPSs)-Opportunities and Challenges for Improving Cyber Security. International Journal of Computer Applications. Published by Foundation of Computer Science (FCS), NY, USA. 2016 March;137(14):19-27.
13. Rekha G, Malik S, Tyagi AK, Nair MM. "Intrusion Detection in Cyber Security: Role of Machine Learning and Data Mining in Cyber Security", Advances in Science, Technology and Engineering Systems Journal. 2020;5(3):72-81.
14. Mishra S, Tyagi AK. "Intrusion Detection in Internet of Things (IoTs) Based Applications using Blockchain Technolgy", Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2019, 123-128. Doi: 10.1109/I-SMAC47947.2019.9032557.
15. Tibrewal I, Srivastava M, Tyagi AK. Blockchain Technology for Securing Cyber-Infrastructure and Internet of Things Networks. In: Tyagi AK, Abraham A, Kaklauskas A. (eds.) Intelligent Interactive Multimedia Systems for e-Healthcare Applications. Springer, Singapore, 2022. https://doi.org/10.1007/978-981-16-6542-4_1
16. Amit Kumar Tyagi, Aswathy SU, Aghila G, Sreenath N. AARIN: Affordable, Accurate, Reliable and Innovative Mechanism to Protect a Medical Cyber-Physical System using Blockchain Technology" IJIN. 2021;2:175-183.