The (In) Security o Smart Cities: Vulnerabilities, Risks, Mitigation and Prevention

Basant Kumar

Abstract*: Smart cities represent the overall development in an urban model utilizing human, and technological enhancement leading to an increase in economic and social opportunities. However, the significant challenges were observed with the rise of smart cities. A comprehensive review is conducted on the study of different approaches used for mitigation of the crime scenarios in smart cities in perspective of hacker's view on hashing and thereby protecting the integrity of the data in heterogeneous devices on a network of smart city. This paper also proposes the ICT architecture of a smart city which is encompassed with numerous security layers in onion model to integrate secure framework for future smart city, for better city living and governance, based on cloud computing IoT and distributed computing in accordance with salted hash value added as a prefix and postfix in a generated password.

Index Terms: encryption, hashing, privacy, smart city, security.

I. INTRODUCTION

Smart cities are the cities that observe and incorporate the status of all their infrastructure management, governance, people and communities, natural environment through information and communication technologies [1].Smart City is a booming universal phenomenon. Smart City refers to an urban transformation using latest ICT technologies, makes cities more efficient and effective.

Internet of things, cyber-physical systems, big data analysis, and real-time control are the techniques used in smart cities [1] to enable intelligent services and provide the comfortable life for localities. Data and connectivity is the basic idea behind smart cities. By using data stream of smart cities i.e. inhabitants location and digital engagement information, transportation etc. are the services which are making smart cities "Smart". Smart city's unsafe applications make people suffer from a series of security and privacy issues. To resolve security and privacy in smart cities, it is a bigger challenge. It becomes utmost necessity to ensure the sensitive data security, cybersecurity and privacy of smart city. A comprehensive approach is used to find out the proposed methods in dealing with the smart city's data security, privacy and trust issues. The people who reside in the smart city use all kinds of electronic devices instead of traditional equipment. The effort in making the smart city to look efficient, the electronic devices should be smart enough to identify the different users [2]. The information security affects a city economically and thus for the better economic development, the challenges in smart city data security and privacy management is to be rectified. The primary sources of data are user-generated contents, surveillance camera and so on. There are different types of crimes related to smart cities. These crimes include data stealing, traffic violation, cybercrime, fraud, theft, violation crimes. Smart surveillance technology or analytics is used to manage the crowd, traffic, cybersecurity, data privacy, and helps in building code to handle disasters etc.

II. BACKGROUND STUDY

68% of the world population projected to live in urban areas by 2050, says UN. Today, 55% of the world's population lives in urban areas, a proportion that is expected to increase to 68% by 2050.

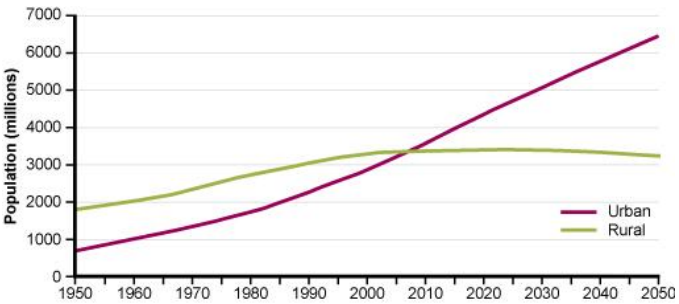

Fig.1- *Urban and rural population of the world*
Source: *Urban and rural population of the world, 1950–2050. (UNDESA, 2014)*

Due to this massive migration problems of access to services that result from rural to urban migration- such as

1. Housing
2. Electricity
3. Shortage of food
4. Shortage of drinking and irrigation water
5. Transportation-traffic (the ability to travel efficiently from one point to another)
6. Sanitation
7. universal access to cleaner energy & sustainable energy
8. Education or Employment
9. Health
10. Ability to manage overall network under an unified system

There is indeed a relationship between the processes of urbanization to the increment of crime rate such as rate of crime in Malaysia particularly in the urban areas is increasing rapidly [41] similarly Australia spent a large

Revised Manuscript Received on July 22 2019.

Basant Kumar, • Professional Ambassador of Oman National CERT, Oman.

amount of money annually in order to tackle the issue of property loss, fraud, emotional cost and others that are related to safety and crime [42].

III. SECURITIES AND PRIVACY ISSUES

The primary security challenges are to protect the data from crime attacks in smart cities by finding the security flaws and preventing the attacks. There are different types of thefts in smart cities and one among which is causing major issue is identity theft where these are the criminal identities who perform the act and has been increased now a days.

The threat matrix as shown in Table I is arranged into several levels of magnitude, where every level is corresponding to distinct sort of threats [3], [4].

Table I: Threat Matrix

Threat Matrix									
Vulnerabilities / Threats	O.S	Application	Network	Firewall	Insecure Wireless	Server	Hardware	Database	Total Score
DOS	✓		✓			✓			3
DDOS	✓	✓	✓	✓		✓			5
SQL Injection		✓						✓	2
Password Attack	✓	✓	✓	✓	✓			✓	5
Cross Site Srcipting (XSS)		✓							1
Phishing		✓							1
Buffer over flow		✓					✓		2
Session Hijacking		✓				✓			2
IP Spoofing			✓	✓					2
Sniffing		✓			✓				2
Man in the Middle			✓	✓				✓	3
Port Scanning			✓						1
Malware threats	✓	✓	✓	✓	✓	✓		✓	7
Total Score	4	9	7	5	3	4	1	4	36

Due to massive presence of threats in current networking environments following potential risks are envisaged and which needs to be addressed.

Table 2: Potential Risks

Smart Services	Potential Risks
E-governance	Citizen personal data, including financial and health data, can be compromised E-governance services can be shut down, denying services to citizens
City surveillance	• Video recordings can be tampered/deleted using SCADA, hampering police investigation
Smart waste management	Smart sewage system can be breached to open/close smart valves and release untreated sewage water into bodies of freshwater A denial of service attack can be performed to interrupt waste collection, posing a risk to citizen health safety
Smart water management	Wrong data related to water management can lead to water shortage
Telemedicine	Citizens' personal/health-related information can be compromised and sold illegally
Intelligent traffic management system	Miscreants can monitor the live location of buses and other parameters to plan an attack Traffic signals can be manipulated to create a traffic jam in the city

Based on several literature reviews and case studies this paper has highlighted some of the dominating factors which will arise as security and privacy issues in smart cities.

A. People and Practices

It is a mutual appreciative that information security heavily depends on the behaviour of the users. Some say information security consists of 20% technical concepts and 80% human behaviour; some say the ratio is 10/90. In an AT&T Network Security survey from March/April 2003[5] Meta Group estimates that "30% of IT security relates to technology, and 70% relates to people and practices".

B. Network Flaws

Networks must be secure as well as functional, and continuously identify vulnerabilities and design metrics to mitigate cyber security threats to networks 19],[27],[15],[28].

Firewalls are an indispensable fragment of network security, and a misconfigured firewall or router can give easy access to an attacker.

Two of the main offenders are dynamic routing, which usually should not be permitted on security devices as best practice, and "rogue" DHCP servers on the network distributing IPs, which can potentially lead to issues of availability as a result of IP conflicts.

C. Vulnerable OS

Windows has the history of flaws and vulnerabilities. If we just want to log on to a system and user doesn't have a password still the user can do various things to find out the password using given tools and techniques

i. Changing the password using CMD
ii. Create a backdoor
iii. Bypassing windows password using konboot
iv. Crack SAM and System using Cain and able
v. Forget Linux Password
vi. Blank SAM database using Kali Linux

D. Hacker's view on Hashing in Application

The integrity of digital data is accomplished by hashing algorithms. In other words, we need a way to verify that the source file is authentic. h=Hx the small x near the capital H is the input data, like an email message, or file, or a password. In general, the purpose of hashing is to add a fingerprint to the piece of data exchanged between a source and a destination.

Hashing is also used in digital signatures, antiviruses capture hashes of files and compare their values with signature definitions. Message Digest version 5, aka MD5, is one of the most popular and fast hashing algorithms and these are widely used in many web application and web sites without realizing the fact it is not good to store password using MD5.

E. Cracking MD5

Hackers apply Hashcat which will load the dictionary file which will take around 2 minutes for SHA-256 to go over all the passwords and run the rule of best 64.

F. Cracking NTLM Hashes

NTLM hashes are stored in the same file located at C, Windows, System32,config. directory. If we try to open it, the operating system will not allow to do it, and hence consequently an error message will be flagged.

Hackers apply a tool called pwdump which will extract the contents of the SAM file where hashes are ready to be cracked. Here hashes are password for one of the admin users on this Windows 7 machine. The important question here is how to protect our accounts from being hacked.

IV. SMART CITY ARCHITECTURE

A distributed Cobit cube security framework called SMARTIE (Secure and smarter ciTIEs data management) for IoT based applications sharing large volumes of heterogeneous information is proposed [22] and the visualization of the smart cities is shown in the below fig 2. End to end security and trust in information delivery is used for decision-making purposes for privacy requirements. The challenges of providing secure exchange of data between IoT devices and providing trust is overcome by SMARTIE framework which is based on an onion model. The salted encryption method is proposed to encrypt password using privacy classification methods under timing constraints selectively. The privacy protection efficiency is achieved. The only limitation to address the practical measurements in real-world evaluations.

It is strongly recommended to classify all components of smart city into specific segments to differentiate and characterize all inputs and outputs of data in a smart city and hence a smart city ICT architecture is proposed in this paper as given in figure 2, which has classified all smart applications under Application layer, data received from heterogeneous devices are kept in Data layer such as big data analytics and predictive modeling oriented data.

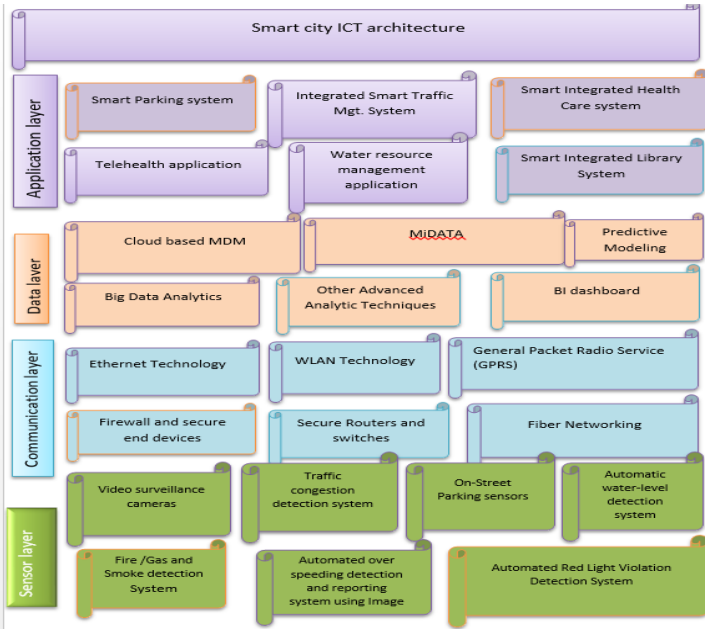

Fig.2- Proposed Smart City ICT Architecture

Network communication based on Ethernet technology or WLAN Technology, firewall, secure routing based packet forwarding and packet switching are categorized under communication layer. It is indeed a fact all IoT based components will be connected to each other and hence all devices based on sensors are placed under sensor layer.

This paper proposes 4 Levels of Smartness

1. Passive : Communicate only when queried (Ex RFID)
2. Active : Communicate when needed (Sensors), Home automation
3. Aware : Action based on simple computations (Ex Tele Health)
4. Autonomous : Can make decisions based on rules (Ex Autonomous cars, Smart Grids)

V. SMART CITY SECURITY SOLUTIONS

We proposed a Security Onion-a kali Linux based Intrusion Detection System on network which can be executed in real time when detection is obtained.

It contains a set of specific tools for security including

i. Snort: packet sniffing
ii. Python: encryption
iii. My sql: storage
iv. Sguil: analyze network events from various utilities
v. Snorby: web-based application for monitoring network security

vi. VGO:traffic analysis
vii. ELSA: for centralized processing system logs and to create reports
viii. Xplico: to recover the data transmitted on the protocols SIP, IRC, HTTP, IMAP, POP, SMTP, FTP,UDP, and others.

The aim of this system is to reduce the time response from administrators to handling system being attack by shutting down the system (Incidence Handling Delay by NIDS).

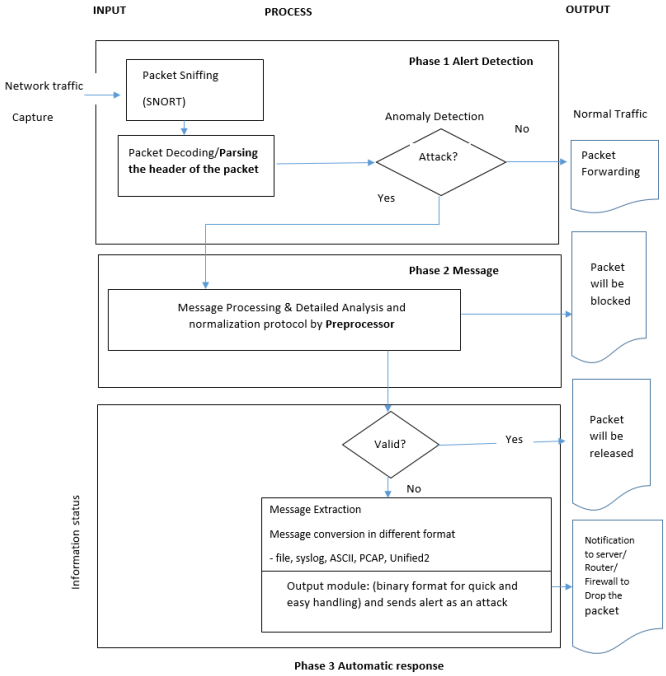

Fig.3- Proposed SNORT based IDs.

In the given figure 3, Security Onion-a kali Linux based Intrusion Detection System is proposed where SNORT is a sensor based packet sniffing device. Once the Packets decoding is done then header of the packets are verified for anomaly detection. If the anomaly is found then it will be sent for detailed analysis by preprocessor

But in case if nothing is found abnormal in packet header then packets will be forwarded further. While doing detailed analysis if once again if nothing is found suspicious based on the behaviors or pattern of the packet then the suspended packet will be released. On the other hand, if the anomaly is tracked then message will be extracted in different format such as syslog, ASCII, PCAP and file and consequently notification is sent to server, router or firewall to drop the packet.

A model and sensor free HVAC (Heating, Ventilation, and Air Conditioning) control algorithm is proposed in [7] which uses simple user input. The iterative data fusion algorithm which saves energy is employed where the temperature of offices with multiple users is taken for comparison. By small increase in temperature, the adaptive HVAC control saves up to 60% of energy. The adaptive HVAC control can save up to 60% energy with a relatively small increase of temperature. To solve many security issues in the cloud a promising cryptographic technique called the attribute-based encryption and thus a framework is proposed for sharing the urban data in [8]. By performance analysis, it is observed that the scheme used is secure and can resist possible attacks. This research was compared with the existing techniques and was found to be more efficient. The intrusion detection systems and intrusion prevention systems are proposed [9] to achieve desired security in the next generation networks. The integrity, confidentiality and availability of cloud services are performed. The adoption of soft computing techniques in IDS/IPS improves security. Further as an advantage to be added, the detection techniques are considered as the trusted platform for the delivery of IoT. The integration of PSR method, the fuzzy logic method for the urban public security evaluation modelling is presented [10]. The challenges of big data in smart cities are multi-dimensional. The public security is ensured by the evaluation index system used in the PSR method. The objective of the entropy model is used for weighing the assignment process. To determine the fuzziness of urban public security the quantitative analysis is performed in a fuzzy method.

A novel data encryption approach named as Dynamic Data Encryption Strategy is proposed in [23]. The method aims to encrypt data using privacy classification methods under timing constraints selectively. The privacy protection efficiency is achieved by following mitigation techniques.

A. Password Security

Passwords should be resilient to physical observation, targeted impersonation, throttled guessing, unthrottled guessing, internal observation, leaks from other verifiers, phishing, and theft; passwords should also be unlinked able and have no trust on third party, and requires explicit consent[13],[14],[15],[16],[17],[6].To store the password securely firstly do not use MD5 or SHA-1.We can use SHA-2 or SHA-3 preferably, and we must check the NIST organization in order to get the latest and greatest hashing algorithms and best practices as well. We should add salting to our hashed password because a hacker could already pre-generate a set of dictionary words and he knows that ABFF56CC is equivalent to 12345, and hence password will be hacked.

B. Data security

Installation of firewalls that is best be application layer gateway firewalls, IDS/IPS, anti-malware, monitoring and encryptions for data-at-rest and on-move that is best be asymmetric or public-key encryption type.

Understand where your data is located, how it flows, and if protected, how it is protected during transmission, business processes and during storage. Understand where your data is located, how it flows, and if protected, how it is protected during transmission, business processes and during storage [18],[19],[20],[21],
22],[28].

C. Encryption

The encryption key should be not less than 2048 bit long, and for symmetric encryption that is single key and mostly used for confidentiality. For hashing like MD7 or SHA-256, encryption key should be not less than 256 bit long, and it best be hardware encryption.[23],[15],[16],[24],[25],[17].

Hashed-based message authenticated code (HMAC) is another hashing algorithm, but this special one requires a secret key to use before applying the hash. What's nice about this algorithm is that it offers integrity and authenticity as well. Email Messaging will be done on heterogeneous mode where senders and receivers will have Encrypted code .Once the message is sent to the receiver where the receiver will receive an OTP on his mobile device which is encompassed with encrypted code and hence even if the email is lost or hacked unless the OTP is not getting verified the mail will not be opened at recipient mode. This methodology will be a milestone in a secure network infrastructure of a smart city.

D. Network Defense using Layers Strategy

Improve industrial control systems cyber security with defense-in-depth strategies using seven layers of protective measures, in a sense that if one fails the other layer takes over as follows, 1) layer 1: Enclaves, which identifies risks and requirement using the "what, how and budget available" to protect, 2) Layer 2: border firewalls, are network/application firewalls that filter known signature attacks, 3) Layer 3: strong authentication, and preferably multi-factor; 4) Layer 4: configuration, and patch management by automating patch, configuration updates and system lockdown, adopting "least privilege, least need to know" to reduce risks of users introducing security flaws, and continually monitoring systems vulnerabilities, 5) Layer 5: host-based firewall, which is more capable of behavior analysis, malicious insiders, and detecting unknown threats and spurious actions and automatically scan files whenever they are opened, copied, moved, saved, or accessed; combined action of both border and host-based firewalls works as intrusion detection and prevention systems . 6) Layer 6: Data encryption, for data at rest that is applied for the whole hard disks including external storage devices, and on-move using secure links. 7) Layer 7: Awareness and training that counter acts social engineering, spam and phishing [7].Prevent man-in-the middle attacks by using VPN, and encrypting data-on-move with either IPsec tunnel mode, SSL, SET or PKI and email encryption like PGP or S/MIME. Also, secure wireless access with WPA PSK/ 20 characters or better.

E. Hardening against IP spoofing

Harden against IP spoofing by, 1) avoiding use of trust relationships only, but a combination of password authentication and trust relationships. 2) Using IPsec, and IP wrappers to allow access only from certain trusted systems. 3) Using random initial sequence numbers (ISN) instead of the regular, predicable sequence numbers. 4) Replacing TCP/IP routing with onion routing that connects users anonymously and encrypted [8].

F. Detection of escalating privileges

Use "booby trapped" session tokens to detect anomaly/misuse to detect authenticated user trying to manipulate tokens to escalate privileges [23].

G. Apply Geographic

Role Based Access Control systems (GEO-RBAC) to deal with the position of mobile users and spatially bounded organizational roles requirements [27].

Detection of insider threats: Introduce unsupervised learning community anomaly detection systems to detect insider threats based on the access logs of collaborative environments [13].

H. Backdoors Detection

Detect backdoors by capturing, 1) rogue accounts, 2) schedule batch jobs, 3) infected startup files, 4) remote control services, 5) monitoring mechanisms, and 6) applications replaced with Trojans [32].

I. Rootkit malware detection and countermeasure

Employ effective tools and techniques for rootkit malware detection and countermeasure [33][34][35].

J. Change-Point Monitoring (CPM) techniques

Apply Change-Point Monitoring (CPM) techniques to detect denial of service attacks, which is based on the inherent network protocol behaviors and instance of the Sequential Change Point, and also it is insensitive to sites and traffic patterns, and a nonparametric Cumulative Sum (CUSUM) method[31].Mobile Ad-hoc Network (MANET) security: Address Mobile Ad-hoc Network (MANET) security, like wormhole attacks, and secure routing protocol Ad-hoc On-Demand Distance Vector (AODV) [36].Defense against browsing history attacks: Apply defense techniques against browsing history attacks via sniffing, user interaction, side channel attacks and interactive techniques [37], [38], [39], [40].

K. Development of secure codes

Focus on improving the software development lifecycle to get programmers to develop cleaner code, by first removing vulnerabilities being attacked and second, creating self-defending codes [41].File checksum: Calculating the file checksum will ensure the integrity and will let us know if someone tampered with the file while downloading a file from the remote machine. Although, before posting the file, the website administrator will calculate the hash of a file and post the hash as an MD5 checksum or SHA checksum and once file is downloaded it will generate another hash to see if it matches the original one posted by the web administrator. If they are equal, then the file is authentic.

VI. ALGORITHM FOR SECURE SECRET KEY (SSK)

It applies a seed value which is called PRNG which stands for PSEUDO RANDOM NUMBER GENERATOR. It is a mechanism for generating random numbers. Many applications on web do not have source of truly random bits and hence PRNG is must to generate random numbers for these all applications. Once the algorithm is used as Pseudorandom function(PRF) to produce a required value such as a session key, then the seed should only be known to the user of the PRF. If the algorithm is used to produce a stream encryption function then the seed has the role of a secret key that must be known the sender and the receiver.

The operation of the algorithms will be

M=[n/outlen] // n=desired no of output bits // hash function has hash value output of outlen bits

```
Data=V                  // V=seed
W=the null string
For i=1 to  m
wi=H(data)              // cryptographic hash function H
W=W || wi

Data=(data+1) mod 2seedlen
//   seedlen=bit length of V ≥ K+64
// Where k is a desired security level expressed in bits
Return leftmost n bits of W
```

Thus, the pseudorandom bit stream is w1 || w2 || w3 ||……. || wm

With the final block truncated if required.

VII. CONCLUSION

This paper reviews the different techniques which have been utilized for addressing data security and privacy. Besides, privacy and security concerns mitigates the crimes seen in Smart cities as these leads to great threats in the integrity of the civic system. Recently, several methods have been developed to protect data and one such is the IoT deployment. The proposed security algorithm **secure secret key** (SSK) will play a significant role in email encryption. However, this approach is found to be complex and requires large research efforts to tackle the challenges in the implementation of the system in real time scenarios. The future work includes the development of Smartie Onion Application - a KALI Linux based distribution on the proposed Onion Security Framework. The system will be primarily used as a software to prevent penetration and block attacks such as the attempts to buffer overflows, hidden port scans, attacks on web application.

REFERENCES

1. Mohanty, S. P., Choppali, U., & Kougianos, E. (2016). Everything you wanted to know about smart cities: The internet of things is the backbone. IEEE Consumer Electronics Magazine, 5(3), 60-70.
2. Ijaz, S., Shah, M. A., Khan, A., & Ahmed, M. (2016). Smart cities: A survey on security concerns. Int. J. Adv. Comput. Sci. Appl, 7(2), pp. 612-625.
3. Thomas, S. R., Veitch, C. K. K. and Woodard, L. , "Categorizing Threat: Building and Using a Generic Threat Matrix.," Sandia Report SAND2007-5791, Sandia National Laboratories, Albuquerque, New Mexico(2007)
4. Mark Mateski, Cassandra M. Trevino, Cynthia K. Veitch, John Michalski, J. Mark Harris, Scott Maruoka, Jason Frye, "Cyber Threat Metrics," SANDIA REPORT, Sandia National Laboratories(2012)
5. Achieving Network Security - An AT&T survey and white paper in cooperation with the Economist Intelligence Unit. 2003
6. OWASP (2017a). White paper: OWASP Top 10 2017. OWASP (USA). Available at: https://www.owasp.org/images/b/b0/OWASP_Top_10_2017_RC2_Final.pdf. Visited on 22nd October 2017.
7. Johnson, Jerry. (2008). Network Defense Requires Layers of Strategic Thinking. Information Week (USA). Feb 25. Iss. 1174, pp. 43 - 49.
8. Fadia, A. (2006). The Unofficial Guide to Ethical Hacking. 2ndedition. Thomson Course Technology (Canada).
9. Shen, J., Liu, D., Shen, J., Liu, Q., & Sun, X. (2017). A secure cloud-assisted urban data sharing framework for ubiquitous-cities. Pervasive and mobile Computing, pp. 219-230.
10. Modi, C., Patel, D., Boris Aniya, B., Patel, H., Patel, A., & Maharajan, M. (2013). A survey of intrusion detection techniques in cloud. Journal of Network and Computer Applications, 36(1), pp. 42-57.
11. Zhou, Q., & Luo, J. (2017). The study on evaluation method of urban network security in the big data era. Intelligent Automation & Soft Computing, pp. 1-6.
12. Tang, B., Chen, Z., Hefferman, G., Wei, T., He, H., & Yang, Q. (2015, October). A hierarchical distributed fog computing architecture for big data analysis in smart cities. In Proceedings of the ASE Bigdata & Social Informatics 2015 (p. 28). ACM.
13. Chen, Y., Nyemba S., and Malin, B. (2012). Detecting Anomalous Insiders in Collaborative Information Systems. IEEE Transactions on Dependable and Secure Computing. IEEE (USA). May/June. Vol. 9, pp. 332-340.
14. Kelley, P., Komanduri, S., Mazurek, M., Shay, R., Vidas, T., Bauer, L., Christin, N., Cranor, L. and López, J. (2012). Guess Again (and Again and Again). Measuring Password Strength by Simulating Password-Cracking Algorithms. 33rd IEEE Symposium on security and privacy (S&P 2012). IEEE computer society (USA).
15. Bonneau, Joseph (2012). The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords. 33rd IEEE Symposium on security and privacy (S&P 2012). IEEE computer society (USA).
16. Panko, R. J. (2011). Corporate Computer and Network Security. 2ndedition. PEARSON (USA).
17. Gellman, D. (2011). Computer Security. rd edition. Wiley (USA).
18. Kanneganti, R. and Chodavarapu, P. (2008). SOA Security. st edition. Manning Publications CO (USA).
19. Norman, S. (2010). Metrics for Mitigating Cyber security Threats to Networks. IEEE Internet Computing. IEEE (USA). January/February. Vol. 14, Iss. no. 1, pp. 64-68.
20. Norman, S. (2010). Metrics for Mitigating Cyber security Threats to Networks. IEEE Internet Computing. IEEE (USA). January/February. Vol. 14, Iss. no. 1, pp.64-68.
21. Skulmoski, Gregory J., Hartman, Francis T. and Krahn, J. (2007). The Delphi Method for Graduate Research. Journal of Information Technology Education. Volume 6, 2007.
22. Jangbok, K., Kihyun, C. and Kyunghee, C. (2007). Spam Filtering With Dynamically Updated URL Statistics. IEEE Security and Privacy. July/August. Vol. 5, no. 4, pp. 33- 39.
23. Jangbok, K., Kihyun, C. and Kyunghee, C. (2007). Spam Filtering With Dynamically Updated URL Statistics. IEEE Security and Privacy. July/August. Vol. 5, no. 4, pp. 33-49.
24. Gai, K., Qiu, M., Zhao, H., & Xiong, J. (2016 June). Privacy-aware adaptive data encryption strategy of big data in cloud computing. In Cyber Security and Cloud Computing (CSCloud), 2016 IEEE 3rd International Conference, pp. 273-278.
25. Hedieh, S. and Mansour, J. (2011). HYSA: Hybrid steganographic approach using multiple steganography methods. Security and Communication Networks. John Wiley & Son Ltd (USA). October. Volume 4. Issue 10, pp. 1173– 1178
26. Gai, K., Qiu, M., Zhao, H., & Xiong, J. (2016 June). Privacy-aware adaptive data encryption strategy of big data in cloud computing. In Cyber Security and Cloud Computing (CSCloud), 2016 IEEE 3rd International Conference on (pp. 273-278). IEEE.Damiani, M. L., Bertino, E. and Perlasca, P. (2007). Data security in location-aware applications. an approach based on RBAC. International Journal of Information and Computer Security (Italy). Vol. 1, No.1/2, pp. 5– 8.
27. Tutton, J. (2010). Incident response and compliance. A case study of the recent attacks. Information Security Technical Report Elsevier Ltd. November. Volume 15, Issue 4, pp. 145- 149
28. ITIL (2011). ITIL standard: ITiL. ITIL (USA). Available at: http://www.itil-officialsite.com/. Visited on: 26th May 2 . Jacobs, David (2012). How to perform a network security audit for customers. TechTarget Inc (USA). Available at: http://searchsecuritychannel.techtarget.com/. Visited on: 27th April 2017.
29. Jung-Shian, L., Che-Jen, H., Chih-Ying, C. and Naveen, C. (2011). Improved IPsec performance utilizing transport-layer-aware compression architecture. Security and Communication Networks. John Wiley & Son Ltd (USA). September. Volume 4. Issue 9, pp. 1063-1065.
30. Haining, W., Danlu, Z. and Kang, G. S. (2004). Change-Point Monitoring for the Detection of DOS Attacks. IEEE Transactions on Dependable and Secure Computing. (USA). October-December. Vol. 1, no. 4, pp. 193-198.
31. McClure, S., Scambray, J. and Kurtz, G. (2012). Hacking Exposed Network Security Secrets and Solutions. th edition. McGraw-Hill/ Osborne (USA).

32. Tsai, J. (2008). Efficient multi-server authentication scheme based on one-way hash function without verification table. Computers and Security. Trustwave (2015). White paper: Web-Application-Firewall. Trustwave Incorporation (USA). May. Volume 27, Issue 3-4, pp. 115-119/.
33. Nitesh, S. and Jonathan, V. (2011). Data remanence effects on memory-based entropy collection for RFID systems. International Journal of Information Security. Volume 10, Number 4, pp. 213-222.
34. Mouza Ahmad, B. S., Chan Yeob, Y. and Mohamed, Jamal Z. (2010). Lightweight mutual authentication protocol for securing RFID applications. International Journal of Internet Technology and Secured Transactions. Vol. 2, No.3/4, pp. 205–222 .
35. Rutvij, H. J., Ashish, D. P., Jatin, D. P. and Bhavin, I. S. (2010). MANET Routing Protocols and Wormhole Attack against AODV. International Journal of Computer Science and Network Security. April. Vol. 10, No. 4, pp. 12- 18.
36. Weinberg, Z., Chen, E., Jayaraman, P. and Jackson, C. (2011). I Still Know What You Visited Last Summer. 32nd IEEE Symposium on security and privacy (S&P 2011). IEEE computer society (USA). pp. 147-151 .
37. Allan, T., Po-WahYau, and MacDonald, John A. (2010). Privacy threats in a mobile enterprise social network. Information Security Technical Report (UK). May. Volume 15, Issue 2, pp. 57 -70. .
38. Baron, L. David. (2010). Preventing attacks on a user's history through CSS. Mozilla (USA).
39. Chunsheng, Liu and Huang, Yu. (2007). Effects of Embedded Decompression and Compaction Architectures on Side-Channel Attack Resistance. IEEE VLSI Test Symposium (VTS'07). pp. 461-478.
40. Robert, W. (2011a). Attackers zero in on Web application vulnerabilities. TechTarget Inc (USA).
41. Sham, R., Omar, N., & Amat, D. W. 2012. Hot Spot Urban Crime Area for Woman Travellers. Procedia - Social and Behavioral Sciences. 68: pp. 417-426.
42. Leden, L., Gårder, P., Schirokoff, A., Monterde-i-Bort, H., Johansson, C., & Basbas, S. 2014. A Sustainable City Environment Through Child Safety and Mobility-A Challenge Based on ITS? Accident; Analysis and Prevention.

AUTHORS PROFILE

I am a research-driven Program Coordinator & Asst. Professor of Master Degree Program in IT and Information security with proven records in enhancing learning environments through hands-on mentorship and differentiated instruction.

- Professional Ambassador of Oman National CERT (http://ambassadors.cert.gov.om/ambassadors_en.aspx)
- Asst. Professor (Computer Science) at MCBS http://www.mcbs.edu.om/en/academics/academic-departments/mathematics-computer-Science/cs-faculty
- EC-Council Certified Ethical Hacker (CEH) certificate no: ECC47685393418
- CompTIA Subject Matter Expert (SME), USA https://certification.comptia.org/get-involved/become-a-subject-matter-expert/current-examplifysmes-
- Officially Designated PhD Guide of Binary University Malaysia for Information Security Program.
- Overseas Examiner of BHARATHIAR University, COIMBATORE, India
- Reviewer of Research Instrument, University Technology Malaysia

EDITORIAL BOARD MEMBER

- Editor in Chief of International Journals of Multidisciplinary Research Academy (IJMRA), https://www.ijmra.us/editor_ijesr.php
- Reviewer of Review of Control Theory and Informatics, PAK Publishing Group, http://www.pakinsight.com/
- Reviewer of American Research Journal of Computer Science and Information Technology. https://www.arjonline.org/engineering-journals/american-research-journal-of-computer-science-and-information-technology/editorial-board