International Journal of Engineering and Information Systems (IJEAIS)
ISSN: 2000-000X
Vol. 2 Issue 12, December – 2018, Pages: 59-66

Use of Blockchain in Strengthening Cybersecurity And Protecting Privacy

Arif Sari
MIS Department, Girne American University
Canterbury, United Kingdom
arifsarii@gmail.com

***Abstract*—*The purpose of this study is to highlight and prove the positive impact in which blockchain could have on today's IoT environment in terms of providing Cybersecurity for not just organizations, but other individuals who share data via the internet. The current IoT environs operates on a centralized cloud based server, meanwhile block chain operates on a decentralized server. The differentiation between the both plays a major role in the level of security they both provide; whereby, decentralized systems are less vulnerable to cyber-attacks and centralized ones are not. In this report, real life illustrations are used to justify the knowledge that the block chain security could serve as a saving grace for internet users. Also, this form of security seems to be the only way to eradicate all forms of insecurity in supply chain and IoT breaches for businesses. An in depth understanding on how the block chain system operates would show why it's held with such high hopes and how it can be beneficial for a wide range of industries. However, this research also highlights some difficulties that might arise in implementing the block chain system. It also gives ways in which the system can be gradually implemented. Firstly, the government needs to make it mandatory for businesses that deal with national based confidential data to implement block chain in their supply chain system to boost security. Secondly, top company officials like C.E. O's need to take genuine interest in the block chain technology by investing in its development and making it a part of employee training, which in the long run would benefit the economy and business in return. Thirdly, a merge of more public and private businesses would help push the use of block chain further. Lastly, the government should make the block chain technology easily accessible, making the official permission to implement -easy and cost effective.*

Keywords—Blockchain, Cybersecurity, privacy, Internet of things, cyber attacks

1. INTRODUCTION

Without a shadow of doubt, eye brow raising tragedies related to poor Cybersecurity has influenced businesses and customers, making them more aware of the high possibility of security breach when personal data or company data is uploaded. With the mentality most customers have now, they hesitate before they put out their information. However, most applications and cloud based networks require this personal information in order to gain users access. Therefore, it becomes a helpless situation for internet users, who have to just comply and hope their information is not being misused. Reason being that Cybersecurity is an alarming issue which constantly poses a threat to the cyber-world. Ironically, this issue happens to be one of the promoting factors for block chain security. It is deemed as a possible rescue against cyber-attacks [1-2].

The block chain technology is a not a new introduction to the cyber world, it was first conceptualized in 1991 but it is just recently gained its popularity amongst people worldwide, especially after the lunch of the cyber currency-bitcoin on its platform. The block chain technology is simply a melting pot whereby transactions are put in form of a puzzle. Users need to agree on a transaction; by making sure that each cryptographic harsh aligns. A cryptographic hash is more or less like a confirmation key. Those confirming this transaction cannot see the details, such as how much wealth the sender or receiver has but they see enough cryptocurrency proof to confirm the validation of the transaction. The application of the block chain technology is endless. It is a secure route in this packed cyber threaten era of the internet. The entire system works with a distributed ledger technology that operates on a decentralized pattern which makes it safe and cost effective because companies don't take the risk alone. Meaning that, other partners are involved in ensuring security through the multiple signature protection.

The behind the scenes logistics seems complicated but executing transactions on this platform is not. The only tasking thing is left to the hackers trying to breach the system. A January 2017 World Economic Forum report predicts that most likely, "by 2025 about Ten percent of global GDP will be stored on block chains or block-related technology." [1-2].

Many Organizations are beginning to gradually implement this system to safeguard data. For example, Guard-time is a software security company that developed a digital signature system based on block chain technology like the company safe guards' data by spreading it all to nodes throughout the system. Therefore, if any hack attempt is made to manipulate data, the whole mass of chains then makes a compassion to metadata packet and then excludes any that do not match up. This makes it almost impossible to hack. Guard-Time has been doing great with this technique as they have worked with reputable companies such as: Sony Ericsson on a cloud computing project [3].

However, many organizations still believe their data can only be secured when the design or implementation of that system is kept a secret- "security through obscurity." Unfortunately, this is not always the case, as we know the tech world is fast developing daily, so is the knowledge of its users- including hackers. Cybersecurity report shows 320% increase hacking attacks in 2016, which is a clear illustration of how dangerous the cyber world is. The bad news for companies relying on security through obscurity; is that once access to the technique of the system is gained by a hacker the whole system is at risk with low chances of rejuvenation [4].

Using Microsoft as an example, when its system was hacked through the use of QAZ Trojan horse which is done when the hacker sends a random email attached with an unseen program. This program enables the hacker control the system of the receiver when the mail is opened, which gives them access to surf through for log in passwords and information. Microsoft security discovered this laps in their security from suspected emails containing several secret passwords used to transfer source codes (languages used to build word and office) from US company's computer to Russia. However, if the implementation of a block chain system was done, they would never have had such problems. A typical example of its excellence is the bitcoin. Although, they have been attempts to hack the system no proven record shows success, no exposure of users' anonymity to hackers of any such [5].

Privacy protection is a pressing issue for a majority of people. As mentioned previously in this research, most people do not want their personal space to be infiltrated and they feel sharing too much personal information would lead to that. Also, most organizations use customer's personal information for secondary purposes which aids to the discomfort of customers to share information on them.

For example, a company that's about to close down, in order to present its self as being expensive for sale it offers its customers information as part of the package that comes with buying the company. (Nigerian ODB Block industries- a construction company. sold 1200 customer information to CEKA insurance LTD when turning over the company. Over 6 customers complained about a new insurance company- ceka, calling their direct lines and showing up at their door steps proposing insurance packages) [6].

Block-chain security is a type of technology that only gives company's access to information the user chooses to share. If customers of ODB companies used this they wouldn't be any infiltration of space. For example, Secure-Key already has experience with this system. The company uses triple blind authentication for its network for over 7 years now. Block chains role for secure-key is to maintain that security but for the sake of identity only whereby no data is being put in the block chain, only evidence of the data.

"There's no personally identifiable information in the block-chain at all. The block-chain is being used for evidence and integrity, not for PII." [7].

Before we dive into other aspects of this research it is important you note that although the popularity of the block chain system is fast growing, there is still no concrete evidence to prove that it would be efficient than the current working system. Reason being that, everything has its pros and cons and most of the block chain cons cannot be pinpointed down at the moment until its fully implemented like the current system – new problems arise every day in the IoT world. Therefore, block-chain eradicating cyber-security is just an optimistic thought judging by its current works.

The relationship between block-chain and cloud computing is one that cannot be easily ignored, the two-work hand in hand with each other. "Cloud computing is simply an information technology paradigm that enables ubiquitous access to shared pools of configurable system resources and higher-level services that can rapidly be provisioned with minimal management effort"- (Wikipedia). Both block chain and cloud were both designed to maximize security, but one just does it better.

2. THE SET UP OF CLOUD AND BLOCKCHAIN AND ITS USES

The setup of the both is different. The cloud adoption is one thing another is to choose which type of cloud to use. It is categorized into public and private clouds. The main difference between these two is that the user is not responsible for any form of management of a public cloud hosting solution. Because the data is stored in the provider's data center and the provider is the one in charge of management of the data center. Organizations use these cloud types depending on the different level of security and management required for that organization, some even use a hybrid cloud.

A public cloud is simply the internet (e.g Google, amazon), a private cloud is dedicated to one organization with strict security controls, it is commonly used amongst medical offices, banking institutions and organizations who are required to meet federal and state guidelines for data controls use, meanwhile, hybrid is a combination of both public and private. (e.g apple
"We use private infrastructure for compute and energy, but we also use public options from AWS, Microsoft Azure and google."- Weinman [2].
Meanwhile, Blockchain can be categorized into the permission and permission-less chain. As the name suggests the permission-less chain requires no acceptance to join, anyone can join e.g. bitcoin. However, the permission chain requires the user to authorize your access, which logically is more secure.

3. SECURITY FOR CLOUD AND BLOCKCHAIN NETWORKS

It shares some similar properties. Blockchain just like cloud, the security of the block model is strong. Cloud constantly monitors suspicious activities in real time - firewall. Which most organizations love to deploy but is not the best option in terms of security because hackers have been successful in the past penetrating these firewalls. On the other hand, block-chain uses cryptographic hash functions which make it almost impossible to hack the entire system. Because once one of the systems is hacked, the hacker still needs to hack all systems connected to that network in order to get full access (and each system needs a key to align). The public and private key cryptography makes sure data is not breached and security in this aspect is quite high [2].

4. CHALLANGES

Cloud networks are not the most trust worthy regardless of the model used, public or private. Its cost of maintenance on the other hand is much, and a common alarming factor of this network is its security and confidentiality. August 2013, demonstrated that no company is safe from hack when the tech giants like Oracle, Sony, T-Mobile and Dropbox dealt with massive hacks and breaches of customer data, and these companies make use of cloud networks [3].

However, block chain has no record of a successful hack. Although the slow deployment of this network is because not too many mechanisms have been invented to support it.

As for cloud networks, it is important to know cyber-attacks are a pressing issue in this tech world and it becomes riskier knowing that, "organizations in most networks run the same code." [3-4].

What the above statement implies is that if hackers get a loop hole that gives them little access to a cloud based network the entire system faces intense risk, therefore increasing the organizations cyber-vulnerability.

In summary, cloud adoption is a strategic move of reducing cost, mitigating risk and achieving scalability of data base capabilities – HCL technologies. This method has some downsides attached to it as mentioned previously therefore it is advisable that organizations should be more conscious of the content they store rather than the medium used in storing this content. Block chain serves as a better option.

5. SECURITY AND PRIVACY IN BLOCKCHAIN - HEALTH CARE INDUSTRY AND MARKET PERSPECTIVE

Without a shadow of doubt the healthcare industry is one that is as important as any top leading industry in a country. Many people flood into hospitals daily. Over 141.4 million people visit the hospital in the space of 5months in the U.S and 7.9% result in hospital admission. This outrageous number would have you thinking how the health care industry keeps its patient's data safe and up-to-date. In the current system, security and trust are the most valuable assets for business; talk less about the health care industry – a more delicate industry dealing with life and death. Information needs to be shared and documented during the line of hospital communication and this leads to trust issues. Many hospitals hold different records of one patient that are not validated, which leads to several errors and incompetency in the health care industry. Between 2005-2001, 140 million patient records were breached according to Protenus Breach Barometer report and it was reported in 2014 that more than 750,000 consumer devices were compromised to distribute phishing and spam emails [5-6].

Having said this, we look into the possible contributions block chain could make in the health care industry in terms of protecting patients' identity and information with its decentralized and encrypted way of sharing, distributing and sharing information which gives maximum security and protects identity.

Speaking of identity, we need to look into the ways in which block chain handles identity exchange compared to the traditional way of identity document exchange in the world [7-9]:

- The typical procedure of this is identifying the person or asset,
- an official government agency approves or notarizes the document
- and lastly an investigation is held on the individual to confirm legitimacy of the money.

However, when it comes to block chain the process is not that tasking. The transfer just involves just two distinct ledgers with a key, one encrypted and the other not. The encrypted key is where you get access to information and it has to be approved for your view by the individual. In block chain this ledger contains all information needed about the individual – it is known as key rings.

"But it's also a problem that looks tailor made for a block chain to solve"- John Halamka chief information officer at Beth Israel Deaconess Medical Centre in Boston.

'The healthcare industry is packed with a lot of cyber related issues. These issues range from malware that compromises the integrity of systems and privacy of patients to distributed denial service (DDos) attacks that disrupt facilities ability to provide health care"- Centre of internet security [10-13].

Critical Healthcare information is often scattered across multiple facilities as mentioned previously. Some of this information need to be retrieved constantly. This process cost money and sometimes even lives. Lack of protection for patient files has been misused. Therefore, better security is needed that's where block chain comes in with its interoperability, integrity, security, and portable user owned data [13-15].

6. ADVANTAGES OF BLOCKCHAIN IN HEALTH CARE AND WHO USES THE SYSTEM CURRENTLY

•Medical records would be accessed securely by authorized persons with permission from provider- saves time, money, duplicated records and most especially lives.

• Those patients who want to give medical records for research purposes can now freely participate without the fear of being known.

• Could help reduce counterfeit drug implications that currently cost pharmaceutical companies and estimated 200 billion dollars yearly.

For example, "Connecting Care is our current revenue-generating, block chain-backed platform," SimplyVital Health CTO Lucas Hendren said in an interview with the author.

"It uses care coordination and financial forecasting to help providers in bundled payments get insight into what happens to patients when they leave the hospital. It is a strategic early use case for block chain in healthcare because it uses block chain as an immutable audit trail." [16-19] .

200 healthcare executives were surveyed and 16 percent say they would adopt the commercial block by the year end. The platforms for this tech are gradually getting available, For example: Block chain Health (San Francisco). Block chain Health is a software company that provides healthcare organizations with HIPAA-compliant block chain solutions.

In conclusion, the advantages to block chain are evident but however, it is a question of if hospitals are ready to adapt to this technology and go against the traditional methods. Are they willing to try workers on how this works?[20-22].

7. BLOCKCHAIN AND IoT SECURITY

Block chain and IoT are two top networks that perfectly complement each other. However, they both have challenges. IoT networks have several loop holes and one major one is its vulnerability to cyber-attacks. IoT hacks are one of the major cyber-attacks that keep companies on their toes. For example, back in October 2016, one of the largest DDoS attack ever was lunched on service provider Dyn using an IoT botnet. This was made possible by a malware called Mirai- (surfs the internet for weak IoT devices and try default usernames and password to login.) Hackers sense vulnerability in an IoT device and they use the front end, back end or middle (Man-in the middle attack) to execute their task. In 2011, tech giants Sony were hit by a security breach by a lone hacker. The hacker infiltrated the network and gained access to 77 million customers info such as usernames, security questions and passwords. Sony's chief information officer (CIO) shinji Hasejima, went to the media to explain the situation. Hasejima believed that the weakest link in Sony's network was the application server and the hacker took advantage of the vulnerability of the company [23-24].

"An application server is a software framework that resides in the middle-tier of a server-centric architecture and provides an environment where an application can run."

Having shown how vulnerable the IoT system is, it is reasonable for companies to seek a new means of protecting data. Which leads us to putting it side by side with the block chain network which could fill up some of its loop holes? However, block chain itself has its own challenges to deal with. This system is not all too new in the industry but its adaptation is a slow process, therefore, they are not too many supporting applications for it. Besides that, block chain is the most appropriate network used in tackling privacy and security problems associated with IoT. In the subsequent explanation, we touch on the mechanisms and key processes that would help achieve a stronger IoT security with block chain.

8. INTEGRATED BLOCKCHAIN IN IoT SECURITY

According to the company's website, "the modum sensors record environmental conditions during shipments. When shipped goods change ownership, the collected data is checked against a specific smart contract in the block-chain. The contract validates that the transaction meets all of the standards set out by the customer, their clients or the regulator and triggers various actions: notifications to sender and receiver, payment, or release of goods, etc."

The above is an example of a company who has deployed the use of block chain in its IoT network in order to transfer of IoT data without central control and management. This makes the entire procedure more secure. Not with holding the fact that to run a block chain is cheaper if integrated into the IoT, it saves the company from cyber-attacks, also time to retrieve files and maintain them.

"Block-chain and IoT together create a 'sweet spot' that form an Internet of Value which allows secure value flow across a range of industry segments," said Cisco Senior Vice President Hilton Romanski. " [25].

The integrated block chain in IoT security makes a stronger network even tech giants like IBM also uses large cloud infrastructure to provide block chain services used to track high value items along the supply chain line. In addition, block chain has

an option of smart contracts for an IoT system. Smart contracts help you exchange money, property, shares or valuable things without the middle man, which means cheaper cost.

For example the company Gartner has estimated that by 2022, so-called ratified unbundled (i.e. defined impact) smart contracts will be in use by more than 25% of global organizations. Companies like IBM and Microsoft word are already ahead in this aspect [26].

In summary, IoT and block chain work better hand in hand with each other. The launch of public block chains like Ethereal and Hyper ledger has enabled more block chain adopters as developers can freely build their own applications on top of them.

9. CENTRALIZED CLOUD MODEL VS DECENTRALISED BLOKCHAIN MODEL

A centralized cloud is one which has a history of security flaws and breaches. As we touched on earlier in this research a decentralized block chain always serves as a better option to avoid these security breaches; however, we must understand how bad the situation with a centralized cloud model is for IoT.

- In 2018, approximately 3.6 billion internet users are projected to access cloud computing services, up from 2.4 billion users in 2013. This serves as concrete evidence that the internet users increase daily. Therefore, companies running on a centralized model transferring confidential information and keeping up with customer demand face great risk of cyber-attacks and increase working cost. Reason being that, the centralized system just needs one access and the whole system can be infuriated. The block chain model would be a better solution in achieving IoT effectiveness.

“Traditional, centralized databases are like castles with moats," said Chronicled CEO Ryan Orr.

"You can fortify them as much as you want, but a hacker will always find a clever way to sneak inside the castle. Block-chain introduces a whole new paradigm. It's a distributed network, data is cryptographically secured, a breach in one node has no effect on the whole, and the consensus mechanism prevents malicious actors from tampering the system. That's one of the things that's really revolutionary about this technology [26].

”

- IoT operate through cloud servers and since users of these network increases daily, some concerns come to mind on how to keep up with the growth. Like any constant growing program or platform – the more users involve, the more capacity needs to be created for them. The IoT is a concept built on networking nodes all linked together via a global network used for (media surfing, streaming, data transfer and so on). As the device grows in reputation amongst people and is being used more than often it becomes harder and expensive to manage communication especially with current centralized model.

“There will be 8.4 billion connected things in 2017, setting the stage for 20.4 billion Internet of Things (IoT) devices to be deployed by 2020, according to analyst firm Gartner. The installed base of hard-to-secure smart things, such as TVs, fridges, and security cameras, is expected to grow 31 percent this year to reach 8.4 billion devices, or around a billion more than the world's total population.” Zdnet [27].

- The centralized cloud model of IoT can be manipulated, which possess a threat to accuracy of information. Whereby, data can be accessed easily. For example, in Nigeria EFCC are responsible for tracking political member’s wealth and tracing its legitimacy, however, the network in which these confidential findings and information are documented are most times manipulated in favor of the politician. This is because third-party-go-betweens are possible. If the system ran on a block chain smart contract where by any found records of looted money automatically triggers an action of the police force.

In conclusion, to get the best security and authorize all information passed through and fro the IoT, block chain technology is the one for the job.

10. BLOCK CHAINS ROLE IN ENSURING SECURITY OF SUPPLY CHAIN

The supply chain is becoming increasingly dependent on secure digital technology. Without a shadow of doubt, supply chain has started tilting towards operating on a more technological level such as the Internet of things (IoT). This is a game changer on how goods are produced and distributed.

For example, global retailer Walmart uses block chain to track scales of pork meat in china. Its processing and storage, and sell-by date. In the event of product recall, the company can also see which batches are concerned and who bought them. Also, with the use of smart contracts deliveries can be made and when not made the system can take action to give penalties or alert to sender.

From conducting payment and audits, to tracing inventory and assets, block chain technology would definitely enable greater supply chain efficiency than ever. With the help of block chain each time a product changes hands it can be documented creating history of the seller to manufacturer of the product. This would save time and cost. Below are the advantages of block chain to supply chain security.

Regardless of the application, block chain offers shippers the following advantages [28]:

- Enhanced Transparency. Documenting a product's journey across the supply chain reveals its true origin and touch points, which increases trust and removes all forms of bias behaviors.

- Better security: due to the use of decentralized and key codes of the block chain better security is being made possible. From a company's stand point, no mix up in data or cyber theft of customer payments etc.

"Many larger producers do not want to reveal provenance of their goods for fear of losing a competitive advantage. Blockchain allows information to be transferred in a trustworthy and anonymous way, essentially providing a trust network that allows information to cascade down the chain from raw material onwards, without revealing who people are." – web magazine innovation enterprise.

- Transparency: take for example the food industry, Blockchain supply chain management programs aim to change the way food is tracked by creating an auditable chain of custody from raw materials to the consumer. Whereby, each step of this requires data to be entered and updated and real time tracing of delivery.

11. BLOCK-CHAIN AND THE FAIR INFORMATION PRACTICES (FIPS)

"Fair Information Practices are a set of principles and practices that describe how an information-based society may approach information handling, storage, management, and flows with a view toward maintaining fairness, privacy, and security in a rapidly evolving global technology environment.".

In the global village in which we live in, information is being uploaded on the internet daily involving confidential messages or public messages. Big data is a pool of these information. Many concerns have arisen over the years regarding the handling of data in big data environment. Most organizations are found guilty to contributing to the misuse of these data. Most organizations take customers information and use them for secondary unauthorized purposes. It almost feels like customers have shown their "nakedness" giving a lot of information up on the internet. Unlike back in those days whereby computers had very little ability to recognize an individual besides their log in used. Meanwhile, now the advancement of technology in IoT enables voice recognition, websites know your biometrics through a wearable device, conversations, best visited sites, etc. Most times this data is stored to help you work faster and feel a sense of ease [29-30].

For example, if an individual visits Facebook daily on his or her system, the system automatically presents an option to save log in details if you agreed on, it then suggests on ways to give the person notifications and keep them involved (reminding about your own birthday even)

Information is power that's why organizations want it. But when it stars becoming an issue is when its misused. Especially when it goes against the fair information conducts.

For example, Acxiom is one of the largest data-brokering firms in the world, is known for collecting data on costumers and selling them to companies. It's an ongoing argument on if its sales of customer information are legal and authorized by the customers [32].

Meanwhile, in China 361 criminal cases came up involving violation of personal data, up from 176 in 2015, said Xie Yongjiang, associate director for the Institute of Internet Governance and Law at the Beijing University of Posts and Telecommunications. Apple on the other hand, were caught up in this scandal in china whereby The Chinese police said Apple contractors had been arrested, 22 of them suspected of selling the personal data of an unspecified number of Apple customers. The police, in Cangnan County in the eastern province of Zhejiang, said the thieves had reaped 50 million renminbi, or about $7.3 million, over an unspecified period [33].

Most customers have their information documented and they have no idea. Block chain technology promises to help solves these issues. With block chain technology data is controlled with private and public keys there is no custodian of user data. The user chooses to whom to release the information to. Also, identification does not need to be an issue; animosity is at its highest [34].

Taking for example the bitcoin, coins containing info, money etc., are transferred from one individual to another without their identity exposed. Same thing would apply to this identification whereby users can log in a system and the owners of the site would have no idea about their identity. Also an audit trail is another block chain feature that would help accountability. Therefore, block chain would essentially help promote fair information practices [35].

12. CONCLUSION

Block chain has proven to be a-go-to tech for better security. The technology would be a challenge for cybercriminals where individuals have control of their own data. Some cloud challenges can be solved through the use of block chain to ensure privacy and security. Its cryptographic verification feature would help stop Mitm. It would help supply chain in terms of cost, speed, safety and transparency. Its function is endless and it can fit in all industries. The future with this technology might solve a lot of problems and also bring about other problems unknown yet.

REFERENCES

[1] Sharma, P.K., Moon, S.Y., Park, J.H., 2017. Block-VN: a distributed blockchain based vehicular network architecture in Smart City. Journal of Information Processing Systems 13 (1), 184–195.

[2] Lee, B., Lee, J.H., 2017. Blockchain-based secure firmware update for embedded devices in an internet of things environment. J. Supercomput. 73 (3), 1152–1167.

[3] Huckle, S., Bhattacharya, R., White, M., et al., 2016. Internet of things, blockchain and shared economy applications. Procedia Computer Science 98, 461–466.

[4] Sari, A.; Rahnama, B., (2013) "Simulation of 802.11 Physical Layer Attacks in MANET," Computational Intelligence, Communication Systems and Networks (CICSyN), 2013 Fifth International Conference on , vol., no., pp.334,337, 5-7 June 2013, http://dx.doi.org/10.1109/CICSYN.2013.79 .

[5] Sari, A., Rahnama, B (2013). "Addressing security challenges in WiMAX environment". In Proceedings of the 6th International Conference on Security of Information and Networks (SIN '13). ACM, New York, NY, USA, 454-456. DOI=10.1145/2523514.2523586 http://doi.acm.org/10.1145/2523514.2523586

[6] Sari, A., Kilic, S., (2017); Exploiting Cryptocurrency Miners with OSINT Techniques, Transactions on Networks and Communications. Volume 5 No. 6, December (2017); pp: 62-76. http://dx.doi.org/10.14738/tnc.56.4083

[7] Sari, A.,, Qayyum, Z.A, Onursal, O. (2017) The Dark Side of the China: The Government, Society and the Great Cannon, Transactions on Networks and Communications. Volume 5 No. 6, December (2017); pp: 48-61. http://dx.doi.org/10.14738/tnc.56.4062

[8] Sari, A. (2017); The Blockchain: Overview of "Past" and "Future", Transactions on Networks and Communications. Volume 5 No. 6, December (2017); pp: 39-47. http://dx.doi.org/10.14738/tnc.56.4061

[9] Sari, A, Akkaya, M., Fadiya, S., (2016) "A conceptual model selection of big data application: improvement for decision support system user organisation" International Journal of Qualitative Research in Services, Vol.2, No.3, pp. 200-210. http://dx.doi.org/10.1504/IJQRS.2016.10003553

[10] Alzubi, A. and Sari, A. (2016) Deployment of Hash Function to Enhance Message Integrity in Wireless Body Area Network (WBAN). Int. J. Communications, Network and System Sciences, Vol.9,No.12, pp. 613-621. http://dx.doi.org/10.4236/ijcns.2016.912047

[11] Sari,A., Akkaya, M. (2016) Contribution of Renewable Energy Potential to Sustainable Employment, Procedia - Social and Behavioral Sciences, Volume 229, 19 August 2016, Pages 316-325, ISSN 1877-0428, http://dx.doi.org/10.1016/j.sbspro.2016.07.142.

[12] Sari, A. Firat, A., Karaduman, A. (2016) Quality Assurance Issues in Higher Education Sectors of Developing Countries; Case of Northern Cyprus, Procedia - Social and Behavioral Sciences, Volume 229, 19 August 2016, Pages 326-334, ISSN 1877-0428, http://dx.doi.org/10.1016/j.sbspro.2016.07.143.

[13] Sopuru, J., Sari, A., (2016) When Technologies Manipulate our Emotions – Smell Detection in Smart Devices. International Journal of Scientific & Engineering Research, Vol.7, No.4, pp. 988-991, ISSN 2229-5518.

[14] Kirencigil, B.Z., Yilmaz, O., Sari, A., (2016) Unified 3-tier Security Mechanism to Enhance Data Security in Mobile Wireless Networks. International Journal of Scientific & Engineering Research, Vol.7, No.4, pp. 1001-1011, ISSN 2229-5518.

[15] Yilmaz, O., Kirencigil, B.Z., Sari, A., (2016) VAN Based theoretical EDI Framework to enhance organizational data security for B2B transactions and comparison of B2B cryptographic application models.International Journal of Scientific & Engineering Research, Vol.7, No.4, pp. 1012-1020, ISSN 2229-5518.

[16] Akkaya, M., Sari, A., Al-Radaideh, A.T., (2016) Factors affecting the adoption of cloud computing based-medical imaging by healthcare professionals. American Academic & Scholarly Research Journal, Vol.8, No.1, pp.13-22.

[17] Sari, A., Onursal, O. and Akkaya, M. (2015) Review of the Security Issues in Vehicular Ad Hoc Net-works (VANET). Int. J. Communications, Network and System Sciences, Vol. 8, No.13, pp. 552-566. http://dx.doi.org/10.4236/ijcns.2015.813050 .

[18] Bal, M., Biricik, C.G. and Sari, A. (2015) Dissemination of Information Communication Technologies: Mobile Government Practices in Developing States. Int. J. Communications, Network and System Sciences, Vol. 8, No.13, pp. 543-551. http://dx.doi.org/10.4236/ijcns.2015.813049.

[19] Cambazoglu, Ş. and Sari, A. (2015) Collision Avoidance in Mobile Wireless Ad-Hoc Networks with Enhanced MACAW Protocol Suite. Int. J. Communications, Network and System Sciences, Vol.8, No.13, pp. 533-542. http://dx.doi.org/10.4236/ijcns.2015.813048.

[20] Sari, A. and Akkaya, M. (2015) Fault Tolerance Mechanisms in Distributed Systems. International Journal of Communications, Network and System Sciences, Vol.8, No.12, pp. 471-482. doi: http://10.4236/ijcns.2015.812042.

[21] Sari, A. and Akkaya, M. (2015) Security and Optimization Challenges of Green Data Centers. International Journal of Communications, Network and System Sciences, Vol.8, No.12, pp. 492-500. doi: http://10.4236/ijcns.2015.812044.

[22] Obasuyi, G. and Sari, A. (2015) "Security Challenges of Virtualization Hypervisors in Virtualized Hardware Environment. International Journal of Communications, Network and System Sciences", Vol.8, No.7, pp. 260-273. doi: http://dx.doi.org/10.4236/ijcns.2015.87026.

[23] Sari, A. (2015) "A Review of Anomaly Detection Systems in Cloud Networks and Survey of Cloud Security Measures in Cloud Storage Applications. Journal of Information Security", Vol.6, No.2, pp. 142-154. doi: http://dx.doi.org/10.4236/jis.2015.62015.

[24] Sari, A. (2015) "Two-Tier Hierarchical Cluster Based Topology in Wireless Sensor Networks for Contention Based Protocol Suite". International Journal of Communications", Network and System Sciences, Vol.8, No.3, pp. 29-42. doi: http://dx.doi.org/10.4236/ijcns.2015.83004.

[25] Sari, A. (2015) "Lightweight Robust Forwarding Scheme for Multi-Hop Wireless Networks". International Journal of Communications, Network and System Sciences, Vol. 8, No.3, pp. 19-28. doi: http://dx.doi.org/10.4236/ijcns.2015.83003.

[26] Sari, A., Rahnama, B., Caglar, E., (2014); "Ultra-Fast Lithium Cell Charging for Mission Critical Applications", Transactions on Machine Learning and Artificial Intelligence, United Kingdom, Vol.2, No.5, pp. 11-18, ISSN: 2054-7390, DOI: http://dx.doi.org/10.14738/tmlai.25.430.

[27] Sari, A. (2014); "Security Issues in RFID Middleware Systems: A Case of Network Layer Attacks: Proposed EPC Implementation for Network Layer Attacks", Transactions on Networks & Communications, Society for Science and Education, United Kingdom, Vol.2, No.5, pp. 1-6, ISSN: 2054-7420, DOI: http://dx.doi.org/10.14738/tnc.25.431.

[28] Sari, A. (2014); "Security Approaches in IEEE 802.11 MANET – Performance Evaluation of USM and RAS", International Journal of Communications, Network, and System Sciences, Vol.7, No.9, pp. 365-372, ISSN: 1913-3723; ISSN-P: 1913-3715, DOI: http://dx.doi.org/10.4236/ijcns.2014.79038.

[29] Megdadi, K., Akkaya, M., & Sari, A. (2018). Internet of Things and Smart City Initiatives in Middle Eastern Countries. In P. Raj, & A. Raman (Eds.), Handbook of Research on Cloud and Fog Computing Infrastructures for Data Science (pp. 289-311). Hershey, PA: IGI Global. ISBN: ISBN13: 9781522559726, doi: https://doi.org/10.4018/978-1-5225-5972-6.ch014.

[30] Rahnama, B., Sari, A., & Ghafour, M. Y. (2016). Countering RSA Vulnerabilities and Its Replacement by ECC: Elliptic Curve Cryptographic Scheme for Key Generation. In D. G., M. Singh, & M. Jayanthi (Eds.) Network Security Attacks and Countermeasures (pp. 270-312). Hershey, PA: Information Science Reference. Doi: https://doi.org/10.4018/978-1-4666-8761-5.ch012

[31] Sari, A., (2015), "Security Issues in Mobile Wireless Ad Hoc Networks: A Comparative Survey of Methods and Techniques to Provide Security in Wireless Ad Hoc Networks", New Threats and Countermeasures in Digital Crime and Cyber Terrorism, (pp. 66-94). Hershey, PA: IGI Global. doi: https://doi.org/10.4018/978-1-4666-8345-7. ISBN: 978146668345, April 2015.

[32] Sari, A., Akkaya, M., Abdalla B., (2017) "Assessing e-Government systems success in Jordan (e-JC): A validation of TAM and IS Success model". International Journal of Computer Science and Information Security, Vol.15, No.2, pp.277-304, ISSN:1947-5500.

[33] Sari, A. (2016); "E-Government Attempts in Small Island Developing States: The Rate of Corruption with Virtualization", Science and Engineering Ethcis, Springer , Vol 23., No. 6, pp.1673-1688, ISSN-O: 1353-3452,DOI: http://dx.doi.org/10.1007/s11948-016-9848-0

[34] Sari, A. (2018) "Context-Aware Intelligent Systems of Fog Computing For Cyber-Threat Intelligence" Springer International Publishing, Springer Book on "Fog Computing: Concepts, Frameworks and Technologies", In: Mahmood Z. (eds). Online ISBN: 978-3-319-94890-4, Print ISBN: 978-3-319-94889-8., doi: https://doi.org/10.1007/978-3-319-94890-4_10.

[35] Sari, A., Alzubi, A., (2017) Path Loss Algorithms for Data Resilience in Wireless Body Area Networks for Healthcare Framework, In Intelligent Data-Centric Systems, edited by Massimo Ficco and Francesco Palmieri, Academic Press, 2018, Pages 285-313, Security and Resilience in Intelligent Data-Centric Systems and Communication Networks, ISBN 9780128113738, doi: https://doi.org/10.1016/B978-0-12-811373-8.00013-6 .