REVIEW OF RESEARCH
IMPACT FACTOR : 5.7631(UIF) UGC APPROVED JOURNAL NO. 48514 ISSN: 2249-894X

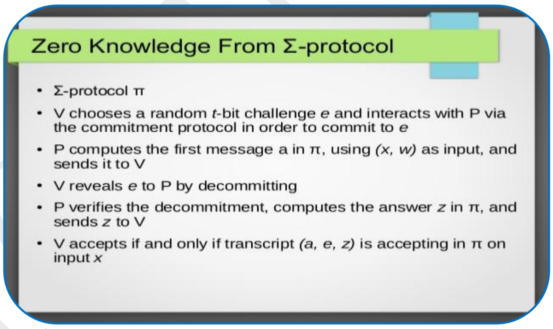
VOLUME - 8 | ISSUE - 6 | MARCH - 2019

COMPARATIVE ANALYSIS OF VARIOUS ZERO-KNOWLEDGE BASED PROTOCOLS UNDER VARIOUS SITUATIONS

Ankur Sodhi[1] and Dr. Rakesh Gangwar[2]
[1] Research Scholar, Department of Computer Science and Engineering, I.K. Punjab Technical University, Kapurthala, Punjab.
[2] Associate Professor, Department of Computer Science and Engineering, Beant College of Engineering and Technology, Gurdaspur, Punjab.

ABSTRACT :

Cryptography is technique for secure communication between two or more parties. There are various techniques available for the same & Zero Knowledge Proof based Protocols is one of them. It is one of the reliable protocols when it comes to authentication & is widely used in various applications. In ZKP the claimant never reveals anything that may reveal the secret. The claimant proves to the verifying party that the secret is known to it, without revealing the secret. The communication between the claimant & verifier is designed in a way that the secret is never revealed. After the message is exchanged the verifier will have the information that whether the claimant is the authentic user or not. In this paper we have discussed the various situations in which the ZKP based protocols are used. There are variety of situations & scenarios where the cryptographic strength of ZKP is used with variations, be if for a Body Wireless Network, for underwater transmission, for cloud computing & at times for providing security for a web-based model. The brief study of various situations in mention in the below stated related work



Zero Knowledge From Σ-protocol

- Σ-protocol π
- V chooses a random *t*-bit challenge *e* and interacts with P via the commitment protocol in order to commit to *e*
- P computes the first message a in π, using *(x, w)* as input, and sends it to V
- V reveals *e* to P by decommitting
- P verifies the decommitment, computes the answer *z* in π, and sends *z* to V
- V accepts if and only if transcript *(a, e, z)* is accepting in π on input *x*

KEYWORDS : *Zero-Knowledge, MANET, Security, Authentication, Clustering .*

RELATED WORK:

In paper **[1]** Changsheng, Vir, Yuzhe&Aiqun (2018) proposed protocols to overcome the issues of Identity-Based Cryptography (IBC) for underwater data transmission. The paper also highlights issues about underwater data transmission. Some of the major issues highlighted are shortage of security infrastructure for underwater wireless communication, vehicle's real identities are transmitted in identity-based cryptographic schemes accompanied with the messages, which results in making it vulnerable to attacks. If real identities are transmitted, the number of vehicles can be counted which are present underwater. We can easily lose the transmitted messages, because of the complex underwater environment. The author has presented two identity-based, non-interactive data transmission protocols. The protocols use a different identity for transmitting of each message & protect their real identities. The count of number of underwater vehicles is protected by using different identities to transmit each message.

In addition, with the proposed identity- based protocols, messages are directly transmitted by underwater vehicles, without sharing any authentication information or key establishment messages which ensures non-interactivity as highlighted in case of IBC. This also saves a lot of energy & in return increases the network lifetime. One can also transmit messages without the information about the other vehicle using one of the proposed protocols which helps in achieving Zero-knowledge & anonymity.

One protocol is based on algebraic signature & other on bilinear map. The protocol based on algebraic signature is suitable in the case of high storage cost but low computation & high storage cost underwater vehicles & Bilinear map-based protocol is suitable for low storage cost & high computation cost underwater vehicles. The analysis & results make a strong case for their use in real world applications. Still, some issues need to be addressed that are discussed in the latter part of this paper.

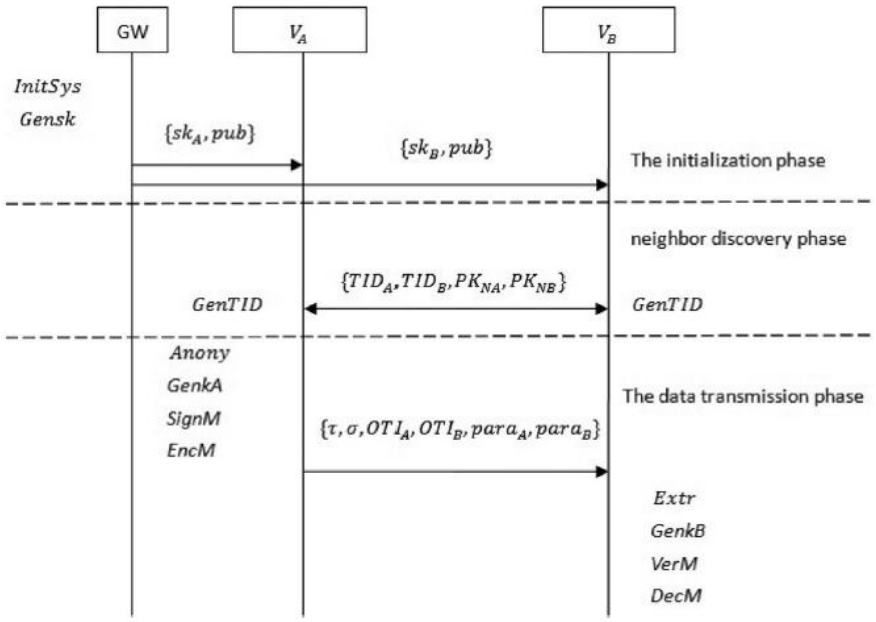


Figure 1 : System model for the two protocols [1]

Based on the changing landscape of technology & a major tilt towards use of IoT to deploy diverse services, Geunil, Bumryoung, & Moon-seog in paper [2] have discussed about one of the most upcoming implementations of IOT technology i.e. z home environment, which is making life a lot convenient & also growing rapidly. One of the major bottlenecks in terms of load burden in smart home environment is on home gateway, which is responsible for authentication in the smart home networks. The secret key of the node is generally used for the authentication in a smart home environment. With the increase in number of nodes, home gateways are under huge burden to manage the secret key of each & every node is also increased. The author has proposed an authentication technique using zero-knowledge proof which will eliminate the reliance of secret key between the home gateway & the node. As the proposed technique doesn't use the secret key the burden on home gateway for managing the secret keys for various nodes is also eliminated.

In the proposed technique, first effort is to distinguish various node in the environment this is achieved in by first exchanging key & after the key exchange has been successfully authenticated the node is registered & identified using the registration protocol. After a node is registered a command & authentication protocol is established using which commands will be delivered via ZKP systems between home gateway & node for any further communications between them.

With the use of IoT technology not being limited to only smart home services but also gaining more applicability in industrial applications as well the need to reduce the burden on gateway becomes more important. The gateway manages & controls lots of nodes (IoT devices). The gateway has secret information of many nodes (IoT devices). A secure communication technique as presented by the author can reduces the burden of gateway using zero-knowledge proof for authentication which eliminates the sharing of secret information of nodes (IoT devices).

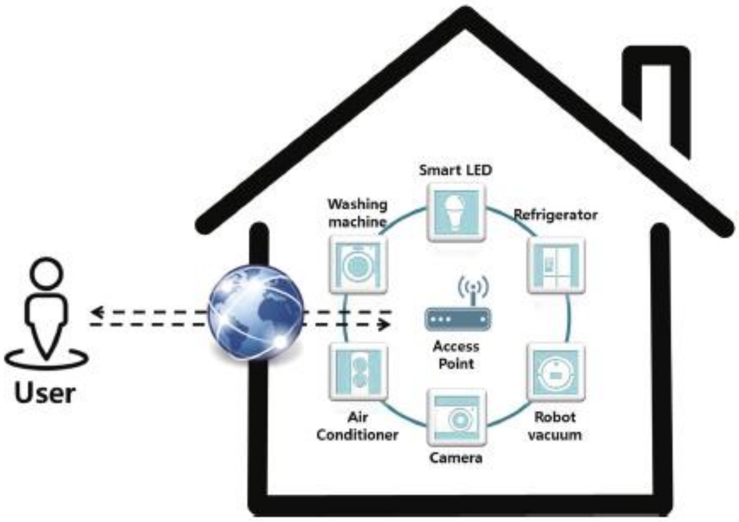


Figure 2 : Smart Home Infrastructure [2]

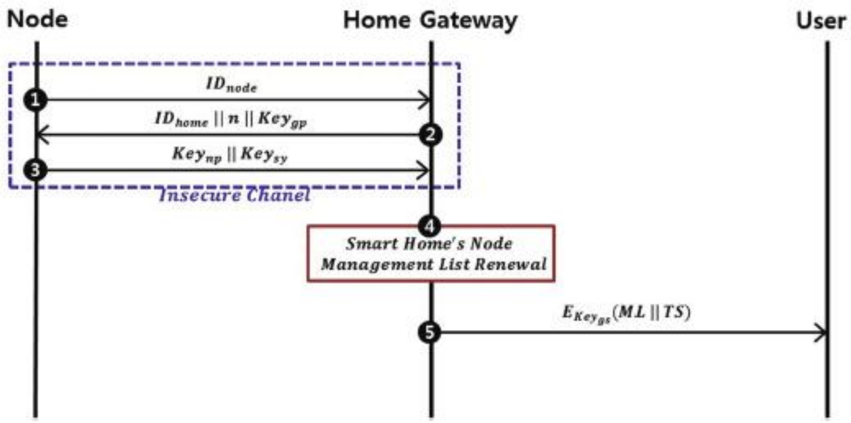


Figure 3: Smart Home Identification & Registration Protocol [2]

The paper [3] the author focused towards block cipher-based identification method using zero-knowledge proof. An information security algorithm is called efficient if it has the two basic attributes: the security it provides & the number of computational resources needed to implement security functions. A major part of computation is involved while adding remote users as more focus must be put on identification & authentication of the user that is being added. As adding of an unwanted user can expose the network to huge risks. In multi-subscriber distributed systems, an important problem is to manage the user authentication & to manage the rights of the user. Because of the type of these specific networks, it is important to have security related protocols which reduce computational complexity to minimum & are robust at the same time.

Earlier work on identification of remote subscriber was directed towards improving the level of security by decreasing the need for communications & improving efficiency. This paper is focused on quick identification of remote users for which the author has proposed the use of zero knowledge strict identification concepts. The result is based on usage of standard block ciphers in contrast to existing methods which use modular arithmetic.

As the proposed solution uses these standard block ciphers which are rigorously tested for cryptographic properties. It may significantly speed up the process of user identification. Along with speeding up of the user authentication process, standard block ciphers also protect against any attempt directed towards the attempt to gain unauthorized access of the resources maintaining high credibility.

Moreover, the theoretical & experimental implementation of the proposed method have proved that fewer computing resources were needed for implementation by using block ciphers property of non-reversible Boolean transformations, in comparison to the methods that use modular arithmetic operations of multiplication. An increase in speed by three orders of magnitude for calculation of an authentication cycle was achieved as compared to existing techniques.

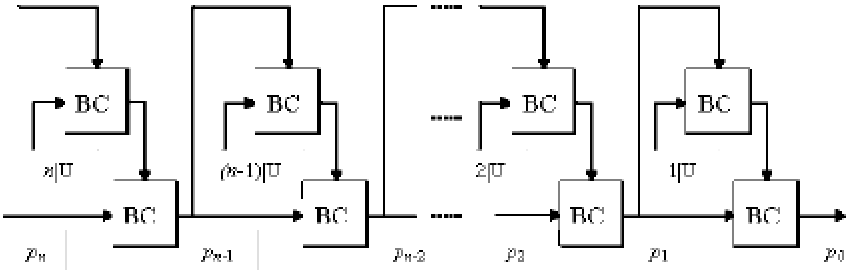


Figure 4: Cryptographic Transformation Architecture in association with the proposed method [3]

In paper [4] the authors collaborated to state that A large number of cyber-attacks are attempted on healthcare facilities. As the records of the patients are of high value & can be leveraged in form of ransomware. Healthcare enterprises are opting for cloud-based solutions to safeguard themselves from such kind of threats & also leveraging the other advantages of cloud computing such as scaling & sharing of risk among stakeholders. Another alternative to cloud that is gaining popularity is fog computing environment & with its growing applications as detailed & discussed in the paper makes it eminent that for environment will be formed. Fog security administration techniques have certain gaps because of which it is currently not adopted for health data. Security provisioning & absence of certification authority (CA) are the major gaps reported. The focus is on the issue of providing a model of impeccable security for medical devices used for fog environments. The proposed model of AZSPM uses the components of atomic security which are composed dynamically. At resident hardware platform, the clock cycles of processor are calculated from service execution for verification & authenticity of the atomic components. A fully sand boxed environment is used for this verification. Ahead of forwarding mobile services to healthcare cloud-lets execution cycles results are evaluated against specifications of service provided by original equipment manufacturer. (OEM) To take care of on-the-fly security policies, a fully distributed ZKP security composition scheme is proposed in paper. The author proposes a dynamic service composition scheme which delivers of the flay certain decentralized security solutions. Security gets delivered by trusted code in fog computation as it is a collection of many cloudlets. Security should be autonomous in a truly distributed environment. Addressing the issues, the proposed AZSPM model which can build the trust between the services with ZKP by which the verifier verifies a cloud service, removing the requirement to develop trust on mobile code. The proposed model can be implemented in Medical Devices & Medical Control Systems in Fog Computing Environments.

Gewu Bu & Maria Potop-Butucaru in paper [5] discussed about Wireless Body Area Networks which is a unique type of Wireless Sensors Network. BAN is different from WSN in a lot of ways. Nodes are spread across the human body in WBAN & move with the body. Due to the mobility, the topology of network in WBAN dynamically changes with the body movement. In WBAN, all the user's data collected by networked body sensors is transmitted to a sink node. Wherever the nodes & their links are highly dynamic the situation is tailor made for multi-hop communication schemes. Lower transmission power is needed for multi-hop communications in comparison to one-hop direct communication. The low transmission power, reduces radio radiation on human body. In WBAN, privacy & security are a major concern in multi-hop communication.

BANZKP combines a ZKP & a Commitment Scheme. Bidirectional authentication (a sender & a verifier) is ensured with the help of Zero Knowledge Proof. Five challenge/response messages are exchanged in BANZKP between the two parties & they never reveal the shared secret. In Commitment Scheme, an encrypted message is transmitted to receiver who doesn't yet have the access to decryption key. The key gets transmitted when the identity of the receiver is proven. Redundancy information crack, DDoS attacks & replay attacks are some of security attacks that BANZKP is vulnerable too. An end-to-end seamless authentication is needed for BANZKP which is not in compliance with the movement of the human posture. BAN-GZKP utilizes two ingredients: hop-by-hop authentication & randomized key allocation. Hop-by-hop scheme of authentication is used in BAN-GZKP which makes it work with postural mobility. The author further provides proof of the steadiness of proposed scheme to various known attacks especially those to which BANZKP is threatened. Moreover, the author substantiates it claim with the help of simulations to prove that BAN-GZKP, outperforms BANZKP on the following network parameters of number of transmissions, end-to-end delay, & packets swapped in network which enhances the reliability to posture mobility of human body. Representative converge-cast strategies was used to compare both the schemes with posture mobility of human body & various transmission rates. BAN-GZKP scheme increases the % of packets received by a significant number, i.e. 34.06%, it further reduced end-to-end-delay by 36.02% & the transmissions went up by 8.75% in comparison to BANZKP. A three-phase authentication is used for BAN-GZKP which is better than BAN-ZKP & that to at no additional cost or overhead on the system.

In paper [6] the authors focused on designing & the implementation of a web security model which will protect the network from attacks. They have used the concept of Diffie-Hellman, Integrity, Confidentiality, Authentication & ZKP to achieve the desired result. The have demonstrated how to successfully handle the Man-In-The-Middle (MITM) attack using ZKP in a web-based security model. In web-based security model the author has worked on 3 layers, namely Client Layer (Web Browser), Server layer & Database layer. The client layer uses a web browser to allow the parties a secret number for authentication. It uses the combination of ZKP, Integrity, Messages & Encryption models to enable authentication. Each message gets concatenated with a HMAC, the resulting data block then gets encrypted using AES. Both the AES & HMAC use the key originating from ZKP

At the server layer the issues between the database & the client interface are addressed. There are following server layer modules

a. ZKP authentication & Key Exchange Module - The module is responsible for Key exchange & ensuring the secret key is not compromised

b. Integrity Module- The module computes message hash & attaches it to the message.

c. Encryption Module - This module encrypts the password using SHA-1 function, also uses AES with the key generated through ZKP

The final layer, i.e. Database layer which takes care of storing information. In this paper it is stated that the web-based security model can fend off the MITM attack using optimized version of ZKP, secret used during the generation of key ensures security.

This paper [7] reveals the concept of device localization which tends to be a very vital functionality for variety of application. **JADE,** the algorithm which is presented in the paper predicts the location of users without considering or having the zero knowledge about the environment surrounded or the number of access points available & this can be done using mmWave communication which reduces the beam training overhead. MmWaves are having short wavelengths & large bandwidth due to which it leads to much denser access points deployment than WIFI. Also, there is presence of different number of mmWave APs, each signal transmitted by the APs take both LoS & NLoS paths to reach a node. This paper's main idea **Joint Anchor & Device location Estimation (JADE)**, which localizes the user & any of the AP that triggers & illuminates it as and when it causes any movement in the indoor space. The Angle-difference-of-arrival (ADoA) algorithm is heart of the localization process, which enjoys leverage due to being invariant to rotation. All the information about components of LoS & NLoS is extracted from spectra of AoA & fed into ADoA algorithm.

Some related works are also considered in this paper, one is Trilateration & Multiliterate but it may route to erroneous location estimate & there is also WIFI-based device localization where the complexity gets delegated to the user device. Other approach is Fingerprint (FP)-based localization scheme, but it is also a non-ideal solution due to the overheads attached to build & maintain a recent and relevant fingerprint database. The proposed solution for the problem is to assume that a deployment of APs in the room at unknown locations. User then is allowed to discover & connect to these APs through either of the two paths available, either LoS or NLoS. The paths are generally revealed using a beam training process which is used in communication systems based of mmWave. With the movement of the user, the AoA of signal from some APs will change, also some APs might vanish behind obstacles, & some others in some time appear again, through either of the two paths, LoS or NLoS. For this, proper notations & geometry functions are considered & also this paper also focused on an optimized algorithm which resulted into the successful completion of the process. This paper also considers the performance of **JADE** based on localization errors. Moreover, the theoretical & experimental implementation of the proposed method have proved that fewer computational resources were required for implementation, the use of mmWave equipment to calculate the information about AoA for various access points using beam training procedures by using the equipment.

In this paper [8] the authors focus on security pertaining to cloud storage. Lot of sensitive data is pushed on the cloud & there emerges the need of trusting the cloud service provider. The paper proposes a scheme based on Interactive Proof Systems named Proof of data possession (PDP). It supports Public verification, improves communication complexity & reduces fraud. The papers deal with the digital content that is stored on Cloud Platform where the problem is with verifying the data Integrity & of untrusted servers. There are numerous attacks against which the protection is required. The PDP scheme has four steps: pre-process, followed by challenge, its proof & then finally verification. The design of the PDP scheme is created using Hash Function. The protocol must fulfil the below mentioned requirements. Public Verifiability, Stateless verification, Low Computation Overhead, Low Communication Overhead, Low storage cost & other unlimited challenges. The security model uses the schemes of GPS which is a ZKP protocol based on public-key which adapts nicely to limited resources. The paper concludes with the proving that the new-ZKP PDP protocol that is the extended version of GPS scheme has high level security & low processing complexity.

Hong Liu & Huansheng Ning in [9] proposed ZKP based Authentication Protocol using an alternative Mode in RFID Systems. RFID represents identification of radio frequency. In ZKAP, dual ZKP is self-assertively picked to deliver anonymity & shared authentication while not revealing any delicate identifiers. Pseudo-irregular banners & access records utilized for quick access & ensure high intensity & quantifiability. Then, formal verification model which is based on reasonable scientific assumptions is built to demonstrate the adapted culmination, zero knowledgeness & soundness & furthermore assault models are embraced to explore versatility & opposition for malignant assaults. It shows that ZKAP claims no undeniable style surrenders on paper & is sufficiently strong to oppose significant assaults like falsification, replay, MITM & interest. The protocol is enticing & material for modest & assets confining RFID systems. Focusing on the ZKP confirmations of ZKAP, within which while working as a prover endeavours to clear authentication by a section protagonist info & aconjointly as a tag prover resolve to clear authentication by a protagonist pursuer. Creators conjointly appear anyway duties & square measure utilized in various modes to deliver signature-based verification alongside shrouded identifiers. Given partner authenticating protocol was created on alternative ZKP mode. Decision confirmation subject integrates with various access the executive components like arbitrary partition, quick check & shared authentication, that is a bonus over general plans. Solid trust is constructed in anonymous air while not revealing any touchy image. Fulfilment, zero-knowledgeness & soundness are accomplished by moderate algebraical assumptions. Various assaults are regularly opposed to reinforce security/privacy protections. In addition, the light-weight protocol accomplishes the wellbeing properties bolstered clear algebraical & coherent operations while not requiring costly logical discipline calculations, & it are frequently quickly authorized in modest & asset confined RFID systems.

In paper [10] Bin Li, Yijie Wang propose associate economical & privacy protective methodology supported the blockchain for clean & fair transactions in shareable economy, alluded to as RZKPB. It stands for Ring SKP which supported the blockchain. RZKPB centres around utilization of e-business dealings inside shareable economy, for e.g. eBay. Right from the start, the blockchain is utilized for recording of every activity of members & grants everyone to learn legitimacy of those activities, that may also work to ensure correctness of transactions in shareable economy. for e.g., the check might happen regardless of whatever the provider provides, i.e. the certifications are that the equivalent of what the customer needs. If off-blockchain, financial debate emerge, fair party will fall back on the chief with these evidences on the blockchain. because of these verifications are confirmed by open. Besides, an exceptional privacy-safeguarding strategy inside the dispersed setting is intended to watch the privacy of transactions from open read while not breaking check convention. In conclusion, tend to don't bring it beyond any doubt parties inside the technique for dealings, that tends to brought together issues simply like a one reason disappointment & accordingly the privacy uncovering. Also, RZKPB depends on a modest presumption that the amount of pernicious members in sharing monetary information proof upheld in the Blockchain, partner practical & privacy defensive ways bolstered the blockchain for honest transactions in shareable economy. the most curiosity of RZKPB lies during a ring zero-information evidence system to watch privacy & ensure that transactions are fair while not breaking the validating convention & including new beyond any doubt party. we achieve the below mentioned points:

(1) Privacy: To maintain the sanctity of the transactions i.e. the privacy, a novel ring zero-information evidence to cover contents of transaction & corporate greed connections while not breaking confirmation on the blockchain.

(2) Fairness: First, verifiers will ensure certificates of provider, that supply is equivalent with the products & meets to needs of customer, that too the correct customer. Secondly, any members can't swindle verifiers during this appropriated setting. Last, all activities will be saved on the blockchain as evidences to determine off-blockchain debate between corporate greed accomplices.

(3) Efficiency: tests are dispensed to experience the off-blockchain & on-blockchain execution of RZKPB. These exploratory outcomes demonstrate that after achieving indistinguishable dimension of security, RZKPB displays higher cryptologic strength than existing 3 privacy-protecting ways.

RZKPB is established first. At that point, each of the provider can enrol their wares on the blockchain. In the event that any customer would love to purchase a merchandise from provider, at that point he receives the arrangement of solicitations from various customer as ring individuals to protect the privacy of corporate greed accomplices. From that point onward, the companion marks an arbitrary cost on client's demand, customer sends encoded dealings parameters to the blockchain for privacy insurance. At that point, provider reacts to demand of customer. Verifiers exclusively secure that the reaction connects to a loop part extraordinary customer rather than a chosen part. In the event that provider & customer have contradictions on their off-blockchain items conveyance, conflict in points of interest can fall back on the administrator with those verifications on the blockchain & result in opening some important parameters. In this case the manager will inflict a penalty on the malignant party & catch individual parameters during intervention. Notwithstanding, this exclusively happens once a corporate greed party carries on malignantly. an affordable related privacy-safeguarding philosophy upholding the blockchain due to honest transactions in shareable economy. RZKPB was proposed to record transactions & incorporate greed connections on blockchain while not uncovering privacy & transferral beyond any doubt party in shareable economy. RZKPB will ensure the legitimacy & privacy of transactions while not harming the confirmation convention during disseminated setting. one tends to experience the online business as partner guide to present RZKPB. in addition, one also experiences the on-blockchain & off-blockchain execution of our centrecytological natives with very surprising settings. It indicates RZKPB will assemble a great deal of conservative transactions contrasted & existing privacy security ways bolstered the blockchain.

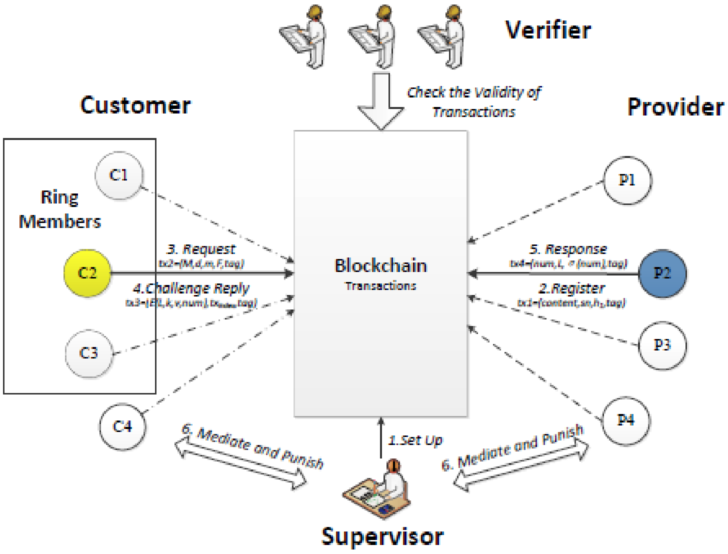


Figure 5: Overview of RZKPB [10]

The paper [11] is mainly focused on secure mechanism which is light weight as well as adaptive in IoT environment which is always a challenge. It uses Multi-graph ZKP based secured authentication system acronym "M-ZAS" that protects IoT devices from various attacks. M-ZAS is divided into four components ***first*** "M-ZKP prover" which not only provides authentication but also adaptive & light-weight, Moreover, it also alleviates huge transmission overheads. ***Second*** *"*M-ZKP verifier" which verifies the impersonator by two methods one by predicting the real provers' secret permutation & other by predicting the challenge sequence.***Third is*** *the* "Adaptive Security Configuration" which gets divided into two derivations, one, security level derivation, which is utilized to establish M-ZKPs soundness probability & other is security level parameter which depicts the parameter utilized in M-ZKP like total number of rounds of attestation. ***Fourth*** is system setup it uses parameter $Sec_{\max}$ for indicating maximum security of M-ZKP

Evaluation of performance was done on the basis of three criteria i.e. communication cost, storage cost & computation cost of M-ZKP & all of these methods are conducted at the similar security level to provide fare & real comparison. As per the observation & experimental results provided by author in context to a particularplatform, total time cost decreases in the case of IoT device comprising of more Public Graphs but in case of M-ZAS any device with low capability which is showing significant improvement has more improvement than with high number of Public graphs which shows M-ZAS can be applied in the IoT devices with low capability.

CONCLUSION & FUTURE WORK:

In paper [1] the author discusses the fact that underwater environment does not have the traditional security features & the signal strength is also quite poor underwater Although 2 protocols are proposed & results show that they are secure & useful in real world, however there are some issues which remain unsolved like how to update the secret keys, how to revoke the keys & how to deal with the cluster heads. In paper [2] the author suggests that many more devices & functionalities can be to IoT devices, but more efficient way to enable secure communication using ZKP is required. In [3] authors conclude that it is proven that the proposed method of Block Ciphers needs fewer computations compared to other known methods. It also states that the feasibility of the scheme using the hardware is yet to be investigated under various conditions. In [4] the author proposes the protocol AZSPM which can be used even if the certification authority is absent. The authors hope that by using the proposed scheme the Interoperability between Healthcare devices in IoT will improve. In [5] the author suggests the improvements over BAN-ZKP. The author highlights the benefits achieved from

BAN-GZKP & states that the results prove the new protocol is more efficient than the previous one. In [6] the author concludes by stating that the proposed ZKP is deterministic with delimited values, that is addresses the issues related to MITM attack & the fact that the keys created in the proposed scheme will be randomized & difficult to detect. In [7] the author has proposed a scheme to map the data in indoor space with the speciality that no prior knowledge of the floor plan, position of nodes & the environment is required. The results show that the JADE algorithm provides accuracy up to 90%. The author suggests the future work to be validating using the real mmWave devices. In [8] the author proposes a scheme based on PDP protocol which uses the positives of elliptic curve variant of the GPS scheme which has benefits of low processing complexity &high-level security. The protocol is more suited to the cloud-basedenvironments. In [9], just like previous papers, the author proposes an alternate Zero Knowledge Scheme where it combines multiple access control mechanisms & achieves the properties of zero knowledge i.e. Completeness, Soundness & Zero-knowledge. The lightweight protocol is well suited for resource-limited RFID environment. In [10] the authors proposed a protocol RZKPB which can be used to record relations & transactions of tradinghappening on the block chain with complete secrecy. The computations suggest that the proposed protocol is better at providing security as compared to the existing techniques for Blockchain. In [11] the author proposes the M-ZAS protocol to safeguard the IoT network from forgery, it suggests that the M-ZAS is a better ZKP authentication-based technique as far as working with IoT is concerned.

REFERENCES

[1] ChangshengWan ,VirViranderPhoha, Yuzhe Tang, and Aiqun Hu, “Non-interactive Identity-Based Underwater Data Transmission With Anonymity and Zero Knowledge” IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 67, NO. 2, FEBRUARY 2018

[2] Geunil Park, Bumryoung Kim, and Moon-seog Jun, “A Design of Secure Authentication Method Using Zero Knowledge Proof in Smart-Home Environment” Springer Nature Singapore 2017 ,J.J. (Jong Hyuk) Park et al. (eds.), Advances in Computer Science and Ubiquitous Computing,Lecture Notes in Electrical Engineering 421, DOI 10.1007/978-981-10-3023-9_35, 2017

[3] Nikolaos G. Bardis, Nikolaos Doukas and Oleksandr P. Markovskyi, “Zero-Knowledge Identification Method based on Block Ciphers” ,2017 International Conference on Control, Artificial Intelligence, Robotics & Optimization,2017

[4] Junaid Chaudhry, Kashif Saleem, Rafiqul Islam, Ali Selamat, Mudassar Ahmad and Craig Valli, “AZSPM: Autonomic Zero-Knowledge Security Provisioning Model for Medical Control Systems in Fog Computing Environments” ,2017 IEEE 42nd Conference on Local Computer Networks Workshops,2017

[5] Gewu Bu and Maria Potop-Butucaru, “BAN-GZKP: Optimal Zero Knowledge Proof based Scheme for Wireless Body Area Networks”,2017 IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems,2017

[6] AmroLouay Al-Bajjari& Ling Yuan, “Research of Web Security Model based on Zero Knowledge Protocol”,7th IEEE International Conference on Software Engineering and Service Science (ICSESS) , IEEE 2016

[7] Joan Palacios, Paolo Casari, Joerg Widmer. “JADE: Zero-Knowledge Device Localization and Environment Mapping for Millimeter Wave Systems”, IEEE INFOCOM 2017 - IEEE Conference on Computer Communications,2017

[8]NesrineKaaniche, Ethmane El Moustaine& Maryline Laurent, ““A Novel Zero-Knowledge Scheme for Proof of Data Possession in Cloud Storage Applications”14th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing,2014

[9]Hong Liu and Huansheng Ning, “Zero-Knowledge Authentication Protocol based on alternative Mode in RFID Systems” IEEE SENSORS JOURNAL, VOL. 11, NO. 12, DECEMBER 2011

[10]Bin Li, Yijie Wang, “ZKPB: A Privacy-protecting Blockchain-Based fair transaction technique for Sharing Economy”17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering,2018

[11] I-Hsun Chuang, Bing-Jie Guo, Jen-Sheng Tsai, Yau-Hwang Kuo1, “Multi-graph Zero-knowledge-based Authentication System in Internet of Things”,IEEE ICC 2017 SAC Symposium Internet of Things Track, 2017

[12] Maryam Shoran and Alex Thomo,”Zero-Knowledge-Private Counting of Group Triangles in Social Networks”,The British Computer Society 2016,29 September 2016

[13] Adam Bouland, Lijie Chen, Dhiraj Holden, Justin Thaler and Prashant Nalini Vasudevan, “On the Power of Statistical Zero Knowledge”,58th Annual IEEE Symposium on Foundations of Computer Science,2017

[14] B.Vijayalakshmi, “A Zero- Knowledge authentication for Wireless Sensor Networks based on Congruence”,2011 Third International Conference on Advanced Computing,IEEE 2011

[15] Nivedita Datta,“Zero-knowledge Password Authentication Protocol”, Advances in Intelligent Systems and Computing, 203: 71-79,2013

[16]Pang Xiyu, Wang Cheng and Zhang Yuhong, “A New P2P Identity Authentication Method Based on Zero-Knowledge under Hybrid P2P Network”, TELKOMNIKA, 11(10): 6187-6192,2013

[17]Ibrahim, M.K., “Modification of Diffie–Hellman Key Exchange Algorithm for Zero Knowledge Proof “, International Conference on Future Communication Networks, 147-152.,2012

[18]QiChengming, “A Zero-Knowledge Proof of Digital Signature Scheme Based on the Elliptic Curve Cryptosystem,” Intelligent Information Technology Application, IITA,: 612-615,2009

[19]Allam A.M, I.I. Ibrahim, I.A. Ali and A.E.H. Elsawy.“Efficient Zero Knowledge Identification Scheme with Secret key exchange”, Circuits and Systems, IEEE, 1:516-519 ,2003

[20]Goldwasser S., Micali S., and Rackoff C., "The Knowledge Complexity of Interactive Proof Systems.” Siam J. Compute, 18(1): 186-208, 1989

[21]Jaramillo C.I., Richard G.G., SperrySean O. and Wayne W.,“An Implementation of a Zero-Knowledge Protocol for a Secure Network Login Procedure,” Proc. Southeastcon ’89 on Energy andI. T. in the Southeast, IEEE, 197-201,1989

Ankur Sodhi
Research Scholar, Department of Computer Science and Engineering,
I.K. Punjab Technical University, Kapurthala, Punjab.

Dr. Rakesh Gangwar[2]
Associate Professor, Department of Computer Science and Engineering,
Beant College of Engineering and Technology, Gurdaspur, Punjab.